

ON THE MARKOFF EQUATION

Norbert Riedel

Abstract A triple (a, b, c) of positive integers is called a Markoff triple iff it satisfies the Diophantine equation

$$a^2 + b^2 + c^2 = abc.$$

Recasting the Markoff tree, whose vertices are Markoff triples, in the framework of integral upper triangular 3×3 matrices, it will be shown that the largest member of such a triple determines the other two uniquely. This answers a question which has been open for 100 years. The solution of this problem will be obtained in the course of a broader investigation of the Markoff equation by means of 3×3 matrices.

Introduction

Markoff numbers, the solutions of the Markoff Diophantine equation, have captured the imagination of mathematicians for over a century. Rooted in A.A. Markoff's late 19th century work on binary quadratic forms and their connection to the top hierarchy of the worst approximable (quadratic) numbers by rationals, these numbers have found their place in seemingly unrelated endeavors of mathematical activity, such as 4-dimensional manifolds ([HZ]), quantum field theory ([CV]), hyperbolic geometry ([Se]), combinatorics ([Po]), group and semi group theory ([Co],[Re]). Two in-depth treatments of the classical aspects of the theory ([Ca], [CF]) bracket almost four decades. One problem that has resisted a conclusive solution so far is the question whether the largest number of a Markoff triple determines uniquely the other two. F.G. Frobenius posed this question in 1913 ([F]). It was restated most recently by M. Waldschmidt in ([W]). A brief discussion of the uniqueness question is included in the exposition of Markoff's theory by E. Bombieri [Bo]. Over the past twenty years various proofs were obtained showing the uniqueness of dominant Markoff numbers which are prime (again, see [Bo] for a survey of the relevant literature). Most of these results, however, seem to be superseded by a far more general result obtained by B. Stolt which was published in 1952 ([St], Theorem 9). The primary objective in the present work is to show that the answer is affirmative throughout, as expressed by the following theorem.

Theorem Given two triples of positive integers, (a_1, b_1, c_1) and (a_2, b_2, c_2) ,

such that

$$a_k < b_k < c_k, \quad \text{and} \quad a_k^2 + b_k^2 + c_k^2 = a_k b_k c_k, \quad k \in \{1, 2\},$$

it follows that $c_1 = c_2$ implies $a_1 = a_2$ and $b_1 = b_2$.

However, since the techniques and formulae leading up to the proof of this statement are far broader than the primary objective itself, a great deal of effort will be dedicated to issues relating to, but not necessarily indispensable for the proof. Hopefully, this broadened approach to the issues involved will contribute to an enhanced understanding of the ideas and the formalism which are so particular to the Markoff equation. The starting point for the proof of the unicity of a dominant Markoff number is to encode every Markoff triple in a (upper) triangular 3x3 matrix, with 1's in the diagonal, and then to determine an explicit form for the "isomorphs" of these matrices. More specifically, given any pair of such matrices, the connectedness of the Markoff tree gives rise to an integral unimodular matrix transforming one into the other, in the same vein as equivalent quadratic forms are related. An integral nilpotent rank 2 matrix, which is associated (essentially uniquely) with each of the aforementioned triangular matrices, gives rise to a one-parameter parametrization of all "automorphs" of those triangular matrices. All of this will be covered in Section 1 through Section 3. The parametrization of the "automorphs" obtained in Section 3 will lead in Section 4 to a diophantine matrix equations, whose solutions are closely related to integers n for which the number -1 is a quadratic residue modulo n . This in turn will lead to a canonical matrix factorization of those solutions which is particular to the Markoff property. In Section 5 the adaptation of this factorization to a slightly more general setting will allow us to settle the proof of the Theorem. In Section 6 we will embark on closer analysis of the matrix which is at the center of the factorization obtained in Section 5. In Section 7 we will draw some number theoretic conclusions which will lead to a further insight into the nature of cycles of reduced indefinite binary quadratic forms containing Markoff forms. Section 8 contains the brief discussion of a norm form equation which depends on a given Markoff number and the affiliated discriminant only, highlighting its connection with the uniqueness question. In Section 9 and Section 10 there will be a discussion of recursions producing data affiliated, and to some degree determined by a given Markoff number. Specifically, in Section 9 we deal with canonical decompositions of the discriminant into sums of two squares, while Section 10 exhibits the algebraic framework in terms of 3x3 matrices for the quadratic residues.

Finally, we note that the theorem above also answers a conjecture by A. N. Tyurin in complex geometry, which is in fact equivalent to it, stating that a representative exceptional bundle on the complex projective plane is uniquely determined by its rank. For details see A. N. Rudakov's article [Ru].

1 Markoff tree and triangular 3x3 matrices

Since the matrix manipulations employed in the sequel render the more common version of the Markoff equation

$$a^2 + b^2 + c^2 = 3abc, a, b, c \in \mathbb{N}$$

impractical, we shall use throughout the alternative form

$$a^2 + b^2 + c^2 = abc,$$

where $a = 3a, b = 3b, c = 3c$. It is also common to represent the three numbers as the components of a triple, arranged in increasing order from the left to the right, for instance. This arrangement is unsuitable for the present purpose. While still referring to this arrangement as a Markoff triple, and the largest number as the dominant member, we will supplement this notion by the following, denoting by $M_n(\mathbb{Z})$ ($M_n^+(\mathbb{Z})$) the set of $n \times n$ matrices whose entries are integers (non negative integers).

1.1 Definition A Markoff triple matrix, or MT-matrix, is a matrix in $M_3^+(\mathbb{Z})$ of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

where $a^2 + b^2 + c^2 = abc$, and $\max\{a, b, c\} \in \{a, c\}$.

For each Markoff triple, with the exception of (3, 3, 3) and (3, 3, 6), there are exactly four MT-matrices. We shall use the notation

$$M(a, b, c) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

for arbitrary entries a, b, c . Throughout this work, a matrix followed by an upper right exponent t denotes the corresponding transposed matrix.

1.2 Proposition For any two MT-matrices $M(a_1, b_1, c_1)$ and $M(a_2, b_2, c_2)$ there exists

$N \in \text{SL}(3, \mathbb{Z})$ such that

a)

$$N^t M(a_2, b_2, c_2) N = M(a_1, b_1, c_1),$$

b)

$$N \begin{pmatrix} c_1 \\ -b_1 \\ a_1 \end{pmatrix} = \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix}, N^t \begin{pmatrix} c_2 \\ a_2 c_2 - b_2 \\ a_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ a_1 c_1 - b_1 \\ a_1 \end{pmatrix}$$

Proof If

$$P(x) = \begin{pmatrix} 0 & -1 & 0 \\ 1 & x & 0 \\ 0 & 0 & 1 \end{pmatrix}, Q(y) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & y & 1 \\ 0 & -1 & 0 \end{pmatrix},$$

then $P(x), Q(y) \in \text{SL}(3, \mathbb{Z})$ for $x, y \in \mathbb{Z}$, and

$$P(a)^t M(a, b, c) P(a) = M(a, c, ac - b)$$

$$Q(c)^t M(a, b, c) Q(c) = M(ac - b, a, c).$$

If $M(a, b, c)$ is a MT-matrix, then the matrices on the right hand side are also MT-matrices, and both are associated with the same neighbor of the Markoff triple corresponding to the MT-matrix on the left hand side. Here the word neighbor refers to two adjacent Markoff triples in the so-called Markoff tree. By the very definition of MT-matrices the Markoff triple associated with the right hand side is further removed from the root of the tree than the corresponding triple on the left hand side. Furthermore, application of transposition and conjugation by

$$\mathcal{J} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

to the two identities above leads to new identities:

$$Q(a)^t M(c, b, a) Q(a) = M(ac - b, c, a),$$

$$P(c)^t M(c, b, a) P(c) = M(c, a, ac - b).$$

So, on the right hand side of these four identities combined, we obtain exactly the four MT-matrices associated with a common Markoff triple. It follows that, through repeated applications of the four identities, the claimed statement is true in case $a_1 = b_1 = c_1 = 3$. Notice that it is vital that there is only one MT-matrix associated with the root of the Markoff tree! The claim in the general case now follows immediately by combining the special case applied to $M(a_1, b_1, c_1)$ and to $M(a_2, b_2, c_2)$ separately.

Remarks 1) The first two of the identities in the proof of Proposition 1.1 give rise to the definition of neighbors in a binary tree with MT-matrices serving as vertices. The Markoff tree, which is not entirely binary, can be recovered from

this tree simply by identifying the four MT-matrices with the Markoff triple they are associated with.

2) If

$$N^t M(3, 3, 3) N = M(a, b, c), N^t \begin{pmatrix} 3 \\ 6 \\ 3 \end{pmatrix} = \begin{pmatrix} c \\ ac - b \\ a \end{pmatrix}, N \in \text{SL}(3, \mathbb{Z}),$$

then

$$N^{-1} M(-3, 6, -3) (N^{-1})^t = M(-a, ac - b, -c).$$

Therefore, if

$$\tilde{N} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} (N^{-1})^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

then

$$(N)^t M(3, 6, 3) \tilde{N} = M(a, ac - b, c), \tilde{N} \begin{pmatrix} c \\ b - ac \\ a \end{pmatrix} = \begin{pmatrix} 3 \\ -6 \\ 3 \end{pmatrix}.$$

Since

$$P(3)^t M(3, 6, 3) P(3) = Q^t(3) M(3, 6, 3) Q(3) = M(3, 3, 3),$$

it follows that, given any two Markoff triples, any permutation of the first, (a_1, b_1, c_1) say, and any permutation of the second, (a_2, b_2, c_2) say, there exists $N \in \text{SL}(3, \mathbb{Z})$, such that

$$N^t M(a_2, b_2, c_2) N = M(a_1, b_1, c_1).$$

3) Markoff triples have also been associated with triples of integral unimodular matrices, exploiting two of the so-called Fricke identities. For an in-depth survey of this approach, mostly due to H. Cohn, see [Pe]. The connection between that approach and the present one is as follows: Let

$$A_0 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } B_0 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

We say that $(A_0, A_0 B_0, B_0)$ is an admissible triple. New admissible triples can be generated out of given ones by the rule, that if (A, AB, B) is an admissible triple, then so are $(A, A^2 B, AB)$ and (AB, AB^2, B) . Fricke's identities ensure that the corresponding triple of traces associated with an admissible triple solves the Markoff equation. Moreover, the lower left entry of each matrix is one-third of its trace. So, once again with the notion of neighbor defined in a natural way, the admissible triples represent nothing but the vertices of the Markoff tree. However, since $(\text{Tr}(A_0), \text{Tr}(A_0 B_0), \text{Tr}(B_0)) = (3, 6, 3)$, the first Markoff triple $(3, 3, 3)$ is missing from the picture. As pointed out in the proof of Proposition

1.2, its availability in the present approach is crucial, due to the fact that it is the only Markoff triple for which all components are equal. Exploiting the fact that a matrix solves its own characteristic equation, one can easily see that each matrix in an admissible triple can be written as a linear combination of the matrices A_0 , A_0B_0 and B_0 with integral coefficients. If $a_2=b_2=c_2=3$ in Proposition 1.2, and if N is the matrix exhibited in its proof, then the coefficient vectors for the admissible triple associated with $(c_1, a_1c_1-b_1, a_1)$ are exactly the columns of the matrix N in the order of their appearance. The 1's in the diagonal of the matrix $M(a_1, b_1, c_1)$ reflect the unimodularity of the 2×2 matrices in the corresponding admissible triple. Other choices for the basis A_0 , A_0B_0 and B_0 appear in the literature, mostly motivated by the desire to connect them to the continued fraction expansion of the quadratic irrationals, which are at the core Markoff's original work. That all these choices are connected via a single integral nilpotent 3×3 matrix, and that this matrix holds the key to the uniqueness question of the Markoff triples, is one of the key observations in the present work.

2. Markoff triples and nilpotent matrices

The statement of Proposition 1.1 raises the issue of “automorphs”, to borrow a notion from the theory of quadratic forms. More specifically, what can be said about the matrices $N \in \text{SL}(3, \mathbb{Z})$ which leave M invariant, i.e.

$$N^t M(a, b, c) N = M(a, b, c)?$$

There are two natural candidates that could serve as generators. While defining them, we will temporarily relinquish the requirement that a, b and c are in \mathbb{Z} . A commutative ring will do. Let

$$H(a, b, c) = M(a, b, c)^{-1} M(a, b, c)^t.$$

If possible, we will suppress the arguments.

2.1 Proposition a) $H^t M H = M$

b) If N is invertible and $N^t M(a_2, b_2, c_2) N = M(a_1, b_1, c_1)$, then

$$N^{-1} H(a_2, b_2, c_2) N = H(a_1, b_1, c_1).$$

Proof a)

$$H^t M H = M(M^{-1})^t M M^{-1} M^t = M.$$

b) Writing

$$M_k = M(a_k, b_k, c_k), H_k = M_k^{-1} M_k^t, k \in \{1, 2\},$$

$N^t M_2^t N = M_1$ implies

$$N^t M_2 N = M_1^t \text{ and } N^{-1} M_2^{-1} (N^t)^{-1} = M_1^{-1},$$

so,

$$N^{-1} H_2 N = N^{-1} M_2^{-1} M_2^t N = N^{-1} M_2^{-1} (N^t)^{-1} N^t M_2^t N = M_1^{-1} M_1^t = H_1$$

□

The explicit form of H is

$$H(a, b, c) = \begin{pmatrix} 1 - (a^2 + b^2 - abc) & ac^2 - bc - a & ac - b \\ a - bc & 1 - c^2 & -c \\ b & c & 1 \end{pmatrix}$$

Its characteristic polynomial is given by

$$\det(H - \lambda E) = -(\lambda - 1)^3 - d(\lambda - 1)^2 - d(\lambda - 1), d = a^2 + b^2 + c^2 - abc$$

Remark The matrix H has a place in quantum field theory ([CV]). More specifically H (or rather its inverse), is the monodromy matrix for the so-called CP^2 σ -model. This is a model with $N=2$ superconformal symmetry and Witten index $n=3$.

The other candidate is related to a matrix $R \in M_3(\mathbb{Z})$ which solves the matrix equation

(2.1)

$$R^t M + M R = 0$$

This matrix is unique up to a multiplicative constant. We can choose

$$R = \begin{pmatrix} a^2 + b^2 - abc & 2a + bc - ac^2 & 2b - ac \\ bc - 2a & c^2 - a^2 & 2c - ab \\ ac - 2b & -2c - ab + a^2 c & abc - b^2 - c^2 \end{pmatrix}$$

Its characteristic polynomial is

$$\det(R - \lambda E) = -\lambda^3 + d(d - 4)\lambda, d = a^2 + b^2 + c^2 - abc$$

In the context of real numbers we can state the following:

2.2 Proposition a) For any $x \in \mathbb{R}$, $(e^{xR})^t M e^{xR} = M$.

b) If (a, b, c) is a Markoff triple, then the adjugated matrix of R , i.e. the transpose of the cofactor matrix, is

$$R^{\text{adj}} = R^2 = 4 \begin{pmatrix} c & & \\ & -b & \\ & & a \end{pmatrix} \begin{pmatrix} c, ac - b, a \end{pmatrix}$$

Proof a) Since $(R^t)^k M = (-1)^k M R^k$ for all $k \in \mathbb{N}$,

$$(e^{xR})^t M e^{xR} = \sum_{k,l=0}^{\infty} \frac{1}{k!} \frac{1}{l!} x^{k+l} (R^t)^k M R^l = \sum_{k,l=0}^{\infty} \frac{1}{k!} \frac{1}{l!} (-1)^k x^{k+l} M R^{k+l} = M e^{-R} e^R = M.$$

b) This can of course be shown through straightforward calculations of the nine minors of R , involving repeated applications of the Markoff property. A more conceptual proof, however, is the following. First one observes that

$$\mathfrak{J}^2 = \mathfrak{J}^{\text{adj}} \text{ for } \mathfrak{J} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Next, the operation of adjugation of a nonsingular matrix commutes obviously with any similarity transformation. Perturbing a singular matrix into a nonsingular one, and then letting that perturbation approach the original matrix shows that adjugation and similarity transformations commute for singular matrices as well. This, once again, settles the claim b).

□

Remark In reference to Remark 3 in Section 1, the conjugation of N by $e^{-\frac{x}{a}R}$ corresponds to the conjugation of the components of the related admissible triple by the matrix

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

The matrices H and R commute, and so they share common eigenvectors. Let us briefly consider R in the context of the ring $P_{\mathbb{Z}}[X]$, the polynomials with integral coefficients. There are exactly two cases in which R is nilpotent, namely $d=0$ and $d=4$. The case $d=0$ leads us to Markoff triples, while the case $d=4$ leads us to triples of Tchebycheff polynomials: For the root of the tree we choose the triple $(X, X, 2)$, X being the free variable. Beginning at the root, we obtain three adjacent (but not necessarily distinct) triples out of a given one, (P_1, P_2, P_3) say, as follows.

$$(P_2 P_3 - P_1, P_2, P_3), (P_1, P_1 P_3 - P_2, P_3), (P_1, P_2, P_1 P_2 - P_3)$$

The polynomials thus obtained are monic polynomials which are mutually orthogonal with respect to a certain probability measure derived from classical potential theory. The triples of integers representing the degrees of these polynomials form the vertices of the so-called “Euclid tree”. While the kinship between the cases $d=0$ and $d=4$ goes well beyond the shared nilpotence of R , a fact which has been exploited by Zagier in [Z] with profit in deriving an asymptotic bound for Markoff numbers through comparison of the two cases, the uniqueness question, which is the subject of the present investigation, has clearly a negative answer in the case $d=4$. The crucial difference between these two cases is the fact that, while R is of rank 2 in the case $d=0$, it is of rank 1 in the case $d=4$. Notice also that, while $H - E$ is nilpotent for $d=0$, it still has two equal but non-vanishing eigenvalues for $d=4$.

From now on we will be exclusively concerned with Markoff triples. Let

$$S = H - E,$$

where E denotes the unit matrix.

2.3 Proposition a) $H = e^{-\frac{R}{2}} = E - \frac{1}{2}R + \frac{1}{8}R^2, R = 3E - 4H + H^2$

b)

$$S^2 = \begin{pmatrix} c \\ -b \\ a \end{pmatrix} \begin{pmatrix} c, ac - b, a \end{pmatrix}$$

The proof is obtained through straightforward manipulations, involving repeated employment of the Markoff property. Proposition 2.3 shows that we are essentially dealing with a single nilpotent matrix of rank 2. It will follow from our subsequent discussion that all “automorphs” have the form e^{sR} for a suitable rational parameter s . Since the matrix R has some mild redundancies, thus making manipulations a bit more lengthy, and since these redundancies are not shared by the matrix S , we will be working in the sequel with S only.

Before we are going to embark on the parametrization of all “automorphs” of the matrices $M(a, b, c)$ via the Jordan normal form, yielding rational matrices which are crucially non-integral, we digress briefly to present a normal form for R which highlights the integrality of the matrix R .

2.4 Proposition a) For each Markoff triple (a, b, c) there exists a matrix $\mathcal{W}(a, b, c) \in \text{GL}(3, \mathbb{Z})$ such that

(2.2)

$$\mathcal{W}(a, b, c)^{-1} \frac{1}{3} R \mathcal{W}(a, b, c) = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

(2.3)

$$\mathcal{W}(a, b, c) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{a} \\ -\mathbf{b} \\ \mathbf{c} \end{pmatrix}, \det(\mathcal{W}(a, b, c)) = -1$$

b) If N is the matrix constructed in Proposition 1.2 for two Markoff triples

(a_1, b_1, c_1) and (a_2, b_2, c_2) then

(2.4)

$$N = \mathcal{W}(a_2, b_2, c_2) \mathcal{W}(a_1, b_1, c_1)^{-1}$$

Proof a) If $(a, b, c) = (3, 3, 3)$, then

$$\mathcal{W}(3, 3, 3) = \begin{pmatrix} 1 & -2 & 0 \\ -1 & 1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$$

has the claimed properties. Now, letting N be the matrix constructed in Proposition 1.2 such that

$$N^t M(a, b, c) N = M(3, 3, 3),$$

then, by Proposition 2.1 b) and Proposition 2.3 a)

$$N^{-1} R(a, b, c) N = R(3, 3, 3).$$

We define

$$\mathcal{W}(a, b, c) = N \mathcal{W}(3, 3, 3).$$

By Proposition 1.2 b), and since $N \in \text{SL}(3, \mathbb{Z})$, the matrix $\mathcal{W}(a, b, c)$ has the claimed properties.

b) This is an immediate consequence of the construction of the matrix N in Proposition 1.2 a). \square

Remark The brevity of the proof of Proposition 2.4 obscures the significance of what's going on here. Some background information might elucidate the issues, especially when this normal form is being compared to the way in which the use of the Jordan normal form unfolds in section 3. First, the normal form enunciated in Proposition 2.4 is essentially unique. In order to clarify this statement one has to place the search for such a normal form on a more systematic footing. Specifically, the proper context for doing so is the Smith normal form for integral matrices. (See for instance [N], Chapter II, for an in depth exposition of this subject). In the case of a 3x3 integral matrix there are exactly 3 determinantal divisors, d_1, d_2, d_3 : d_1 is the greatest common divisor of all nine matrix entries, d_2 is the greatest common divisor of all nine entries in the corresponding adjugated matrix, and d_3 is the determinant of the

given matrix. For a nonsingular integral 3x3 matrix the Smith normal form is then given by $\text{diag}(d_1, \frac{d_2}{d_1}, \frac{d_3}{d_2})$, and for a singular integral 3x3 matrix of rank 2 it is given by $\text{diag}(d_1, \frac{d_2}{d_1}, 0)$. The diagonal entries in the Smith normal form are called the invariant factors of the matrix. The Smith normal form is known to be invariant under left as well as right multiplication by unimodular integral matrices. In our case one can see that the matrix $\mathcal{R} = \frac{1}{3}R$ has the Smith normal form $\text{diag}(1, 4, 0)$. Indeed, the first determinantal divisor of \mathcal{R} is equal to 1 (for instance the greatest common divisor of the entries (1,1), (1,2) and (3,3) is equal to 1), by Proposition 2.2(b) the second determinantal divisor of \mathcal{R} is equal to 4, and finally, $\det(\mathcal{R}) = 0$. By [Ne], Theorem III.12 there exists a matrix $\mathcal{W} \in \text{GL}(3, \mathbb{Z})$, such that

$$\mathcal{W}^{-1}\mathcal{R}\mathcal{W} = \begin{pmatrix} 0 & \alpha & \beta \\ 0 & 0 & \gamma \\ 0 & 0 & 0 \end{pmatrix} \in \mathbf{M}_3(\mathbb{Z}).$$

By [AO], section 11, we may assume that

$$\alpha > 0, \gamma > 0, \text{ and } 0 \leq \beta < \gcd(\alpha, \gamma),$$

rendering this choice unique in the sense that any two similar matrices of this form must be identical (see [AO], section 12). The only non-vanishing cofactor in the upper triangular matrix is the one with index (1,3). Since the second determinantal divisor of \mathcal{R} is equal to 4, we conclude that $\alpha\beta = 4$. This in turn entails that

$$\mathcal{W}^{-1}\mathcal{R}\mathcal{W} \in \left\{ \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 4 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \right\}.$$

In order to show that only the first matrix can occur, we note that, on the one hand both, \mathcal{R}

and $\begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$ are similar (with respect to $\text{GL}(3, \mathbb{Z})$) to the negative of their transposed matrix.

In the first case this follows from (2.1), and in the latter case we have

$$\begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} = - \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 2 & 0 \end{pmatrix}.$$

On the other hand, conjugating the matrix $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}$ to the negative of its transposed,

$$X \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} X^{-1} = - \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix},$$

leads to a matrix of the form

$$X = \begin{pmatrix} 0 & 0 & -4x \\ 0 & x & y \\ -4x & -y & z \end{pmatrix}; x, y, z \in \mathbb{Z}.$$

Since the determinant of this matrix is $-16x^3$, X can never be chosen to be unimodular. Since

$$\begin{pmatrix} 0 & 4 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \mathcal{J} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}^t \mathcal{J},$$

the matrix $\begin{pmatrix} 0 & 4 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ too is not similar to the negative of its transposed via an integral unimod-ular matrix. Finally, since the property of a matrix to be similar to the negative of its transposed is invariant under similarity transformations, there has to exist a matrix $\mathcal{W} \in \text{GL}(3, \mathbb{Z})$ such that

$$\mathcal{W}^{-1} \mathcal{R} \mathcal{W} = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

as claimed in Proposition 2.4. Up to this point (2.2) and (2.3) follow, except for the sign of the determinant of the matrix \mathcal{W} . What is not obtainable through this line of reasoning, however, is (2.4). The best one can get is

$$N = \mathcal{W}(a_2, b_2, c_2) \mathcal{W}(a_1, b_1, c_1)^{-1} + \varepsilon \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} \begin{pmatrix} c_1, a_1 c_1 - b_1, a_1 \end{pmatrix},$$

with an unspecified integer ε . Notice that the value of ε does not change if any of the matrices \mathcal{W} is multiplied from the left by a matrix with determinant 1 which commutes with the corresponding nilpotent matrix R .

3 Determination of automorphs

There are two objectives in this section. First we seek to develop a one-parameter characterization of the “automorphs” introduced in the previous section. Second, this should be done in a way so that the formulas that will be the point of departure in the the next section emerge in a natural way from the ones we obtain in the present one. In order to meet those two requirements, we shall, for the most part in this section, work with two Markoff triples which share a common member. First we construct a matrix T which conjugates S to

its Jordan form. Starting with an eigenvector for S^t yields

$$S \begin{pmatrix} c \\ ac-b \\ a \end{pmatrix} = ac \begin{pmatrix} ac^2-bc-a \\ -c^2 \\ c \end{pmatrix}$$

Notice that the vector on the right hand side is nothing but the second column of S multiplied by ac . Applying S to its second column yields by virtue of the Markoff property

$$(ac-b) \begin{pmatrix} c \\ -b \\ a \end{pmatrix},$$

which is in the kernel of S . So, if we define

$$T = \begin{pmatrix} c & ac(ac^2-bc-a) & ac(ac-b)c \\ ac-b & ac(-c^2) & ac(ac-b)(-b) \\ a & acc & ac(ac-b)a \end{pmatrix}$$

then we have

$$ST = T \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Furthermore,

$$\det(T) = -[ac(ac-b)]^3$$

In order to manage the manipulations involving this matrix efficiently, we will use a suitable factorization. If

$$A = \begin{pmatrix} 0 & c(ac-b)-a & c \\ 1 & -c^2 & -b \\ 0 & c & a \end{pmatrix},$$

$$B = \begin{pmatrix} ac & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & ac & 0 \\ 0 & 0 & ac(ac-b) \end{pmatrix},$$

then $T = ABCD$. Moreover

$$A^{-1} = -\frac{1}{(ac-b)^2} \begin{pmatrix} -c(ac-b) & -(ac-b)^2 & -a(ac-b) \\ -a & 0 & c \\ c & 0 & a-c(ac-b) \end{pmatrix}$$

$$= \frac{1}{(ac-b)^2} FKL,$$

where

$$F = \begin{pmatrix} ac-b & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$K = \begin{pmatrix} c & 1 & a \\ a & 0 & -c \\ -c & 0 & c(ac-b)-a \end{pmatrix}$$

$$L = \begin{pmatrix} 1 & 0 & 0 \\ 0 & ac-b & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We shall also need the matrix

$$U = MT = VBCD,$$

where

$$V = \begin{pmatrix} a & -a & c \\ 1 & 0 & m \\ 0 & c & a \end{pmatrix}$$

$$V^{-1} = \frac{1}{(ac-b)^2} \begin{pmatrix} c(ac-b) & -b(ac-b) & a(ac-b) \\ a & -a^2 & a(ac-b)-c \\ -c & ac & -a \end{pmatrix}$$

Now consider two Markoff triples (at this point not necessarily distinct) with a common member m . We assume that

$$m = a_1c_1 - b_1 = a_2c_2 - b_2,$$

where a_k , b_k and c_k are the components of the unique neighbor closer to the root of the Markoff tree, for $k = 1$ and $k = 2$, respectively. This arrangement accommodates all vertices of the Markoff tree except for the root. In order to make use of the matrices introduced above in the present context, we adopt the convention of attaching an index 1 or 2 to their names, depending on the Markoff triple in reference. Let

$$N = T_2T_1^{-1}, r = \frac{a_1c_1}{a_2c_2}.$$

Then

$$\det(rN) = 1$$

By Proposition 1.1 there exists a matrix $N \in \text{SL}(3, \mathbb{Z})$ such that

(3.1)

$$N^t M(a_2, b_2, c_2) N = M(a_1, b_1, c_1).$$

By Proposition 2.1(b)

$$N^{-1}S_2N = S_1$$

Since $(N)^{-1}S_2N = S_1$, it follows that $N(N^{-1})^{-1}$ and S_2 commute. Since S_2 has rank 2, this implies that there exist rational numbers s and t , such that

(3.2)

$$N = r(E + sS_2 + tS_2^2)N = rT_2 \begin{pmatrix} 1 & 0 & 0 \\ s & 1 & 0 \\ t & s & 1 \end{pmatrix} T_1^{-1} \epsilon \mathbf{M}_3(\mathbb{Z}).$$

Substituting (3.2) into (3.1) yields the identity

(3.3)

$$r(T_1^t)^{-1} \begin{pmatrix} 1 & s & t \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} T_2^t = r^{-1} (M(a_2, b_2, c_2) T_2 \begin{pmatrix} 1 & 0 & 0 \\ s & 1 & 0 \\ t & s & 1 \end{pmatrix} (M(a_1, b_1, c_1) T_1)^{-1})^{-1} =$$

$$r^{-1} U_1 \begin{pmatrix} 1 & 0 & 0 \\ -s & 1 & 0 \\ s^2 - t & -s & 1 \end{pmatrix} U_2^{-1}$$

We are now going to evaluate the three terms in (3.2). Writing F, L in place of F_1, L_1 , respectively,

$$rm^2 N = r A_2 B_2 C_2 D_2 D_1^{-1} C_1^{-1} B_1^{-1} F K_1 L =$$

$$A_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{a_2 c_2} - \frac{1}{a_1 c_1} & 0 & 1 \end{pmatrix} F K_1 L =$$

$$\begin{pmatrix} c_2(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1})m & c_2 m - a_2 & c_2 \\ (1 - b_2(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}))m & -c_2^2 & -b_2 \\ a_2(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1})m & c_2 & a_2 \end{pmatrix} K_1 L =$$

$$\Gamma_0 + m\Gamma_1 + m^2\Gamma_2,$$

where,

$$\Gamma_0 = \begin{pmatrix} -(a_1 a_2 + c_1 c_2) & 0 & -(a_1 c_2 - c_1 a_2) \\ -(a_1 c_2 - c_1 a_2) c_2 & 0 & (a_1 c_2 - c_1 a_2) a_2 \\ a_1 c_2 - c_1 a_2 & 0 & -(a_1 a_2 + c_1 c_2) \end{pmatrix}$$

$$+ m \begin{pmatrix} a_1 c_2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & c_1 a_2 \end{pmatrix}$$

$$\Gamma_1 = (\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}) \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} (c_1, m, a_1)$$

$$\Gamma_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Since

$$m^2 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} T^{-1} = a^{-1} c^{-1} \begin{pmatrix} 0 & 0 & 0 \\ m & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} KL = a^{-1} c^{-1} L \begin{pmatrix} 0 & 0 & 0 \\ c & 1 & a \\ a & 0 & -c \end{pmatrix} L,$$

we get for the second term

$$mrS_2 N^\sim = mrT_2 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} T_1^{-1} = A_2 \begin{pmatrix} 0 & 0 & 0 \\ c_1 & 1 & a_1 \\ a_1 & 0 & -c_1 \end{pmatrix} L =$$

$$\Omega_0 + m\Omega_1,$$

where

$$\Omega_0 = \begin{pmatrix} a_1 c_2 - c_1 a_2 & 0 & -(a_1 a_2 + c_1 c_2) \\ -(a_1 a_2 + c_1 c_2) c_2 & 0 & -(a_1 c_2 - c_1 a_2) c_2 \\ a_1 a_2 + c_1 c_2 & 0 & a_1 c_2 - c_1 a_2 \end{pmatrix},$$

$$\Omega_1 = \begin{pmatrix} 0 & -a_2 & 0 \\ a_1 & -c_2^2 & -c_1 \\ 0 & c_2 & 0 \end{pmatrix} + c_2 \begin{pmatrix} c_1 & m & a_1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Finally, for the third term

$$rS_2^2 N^\sim = \Phi^t = \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} (c_1, m, a_1).$$

In order to manipulate the identity (3.3) we shall need a similar decomposition involving the matrix U .

$$r^{-1} m^2 U_1 U_2^{-1} = V_1 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}) & 0 & 1 \end{pmatrix} \begin{pmatrix} c_2 m & -b_2 m & a_2 m \\ a_2 & -a_2^2 & a_2 m - c_2 \\ -c_2 & a_2 c_2 & -a_2 \end{pmatrix}$$

$$= \Theta_0 + m\Theta_1 + m^2\Theta_2,$$

where

$$\Theta_0 = \begin{pmatrix} -(a_1 a_2 + c_1 c_2) & -(a_1 c_2 - c_1 a_2) c_2 & a_1 c_2 - c_1 a_2 \\ 0 & 0 & 0 \\ -(a_1 c_2 - c_1 a_2) & (a_1 c_2 - c_1 a_2) a_2 & -(a_1 a_2 + c_1 c_2) \end{pmatrix}$$

$$+ m \begin{pmatrix} a_1 c_2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & c_1 a_2 \end{pmatrix},$$

$$\Theta_1 = -\left(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}\right) \begin{pmatrix} c_1 \\ m \\ a_1 \end{pmatrix} \begin{pmatrix} c_2, -b_2, a_2 \end{pmatrix},$$

$$\Theta_2 = \Gamma_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Since

$$m^2 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} U^{-1} = a^{-1} c^{-1} \begin{pmatrix} 0 & 0 & 0 \\ cm & -bm & am \\ a & -a^2 & am - c \end{pmatrix},$$

we get

$$\begin{aligned} r^{-1} m U_1 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} U_2^{-1} &= V_1 \begin{pmatrix} 0 & 0 & 0 \\ c_2 & -b_2 & a_2 \\ a_2 & -a_2^2 & a_2 m - c_2 \end{pmatrix} \\ &= \Lambda_0 + m \Lambda_1, \end{aligned}$$

where

$$\begin{aligned} \Lambda_0 &= \begin{pmatrix} -(a_1 c_2 - c_1 a_2) & (a_1 c_2 - c_1 a_2) a_2 & -(a_1 a_2 + c_1 c_2) \\ 0 & 0 & 0 \\ a_1 a_2 + c_1 c_2 & -(a_1 a_2 + c_1 c_2) a_2 & -(a_1 c_2 - c_1 a_2) \end{pmatrix}, \\ \Lambda_1 &= \begin{pmatrix} 0 & -a_1 & 0 \\ a_2 & -a_2^2 & -c_2 \\ 0 & c_1 & 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 & 0 & c_1 \\ 0 & 0 & m \\ 0 & 0 & a_1 \end{pmatrix}. \end{aligned}$$

Finally,

$$r^{-1} U_1 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} U_2^{-1} = \Phi$$

Let

(3.4)

$$\begin{aligned} N(s) &= r e^{-\frac{R_2}{2}s} N^\sim - \frac{1}{m} \left(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1} \right) \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} \begin{pmatrix} c_1, m, a_1 \end{pmatrix} = \\ &= r N^\sim e^{-\frac{R_1}{2}s} - \frac{1}{m} \left(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1} \right) \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} \begin{pmatrix} c_1, m, a_1 \end{pmatrix} \end{aligned}$$

Then we have the following crucial representation of all “rational isomorphs”.

3.1 Proposition If $Q \in \text{SL}(3, \mathbb{Q})$, then

(3.5)

$$Q^t M_2 Q = M_1,$$

if and only if there exists a rational number s such that $Q = N(s)$.

Proof First, by our discussion above, we know that if (3.5) holds true, then there exist rational numbers s and t , such that

$$Q = r(E + sS_2 + tS_2^2)N.$$

Now given this representation, Q satisfies (3.5) if and only if

$$(3.6) r(T_1^t)^{-1} \begin{pmatrix} 1 & s & t \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} T_2^t - r^{-1} U_1 \begin{pmatrix} 1 & 0 & 0 \\ -s & 1 & 0 \\ s^2 - t & -s & 1 \end{pmatrix} U_2^{-1} = 0.$$

Employing the above decompositions, the left hand side of (3.6) turns into

$$\frac{1}{m^2} \Gamma_0^t + \frac{1}{m} \Gamma_1^t + \Gamma_2^t + \frac{s}{m} \Omega_0^t + s \Omega_1^t + t \Phi - \frac{1}{m^2} \Theta_0 - \frac{1}{m} \Theta_1 - \Theta_2 + \frac{s}{m} \Lambda_0 + s \Lambda_1 - (s^2 - t) \Phi.$$

Since

$$\Gamma_0^t = \Theta_0, \Gamma_1^t = -\Theta_1 = \left(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}\right) \Phi, \Gamma_2^t = \Theta_2,$$

the left hand side of (3.6) simplifies to

$$\frac{s}{m} (\Omega_0^t + \Lambda_0) + s (\Omega_1^t + \Lambda_1) + \left(2 \left(\frac{1}{m} \left(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}\right) + t\right) - s^2\right) \Phi.$$

But

$$\Omega_1^t + \Lambda_1 = \Phi + \begin{pmatrix} 0 & c_1 b_2 & 0 \\ 0 & 0 & 0 \\ 0 & a_1 b_2 & 0 \end{pmatrix},$$

while

$$\Omega_0^t + \Lambda_0 = -m \begin{pmatrix} 0 & c_1 b_2 & 0 \\ 0 & 0 & 0 \\ 0 & a_1 b_2 & 0 \end{pmatrix},$$

so that the left hand side of (3.6) finally takes the form

$$\left(2 \left(\frac{1}{m} \left(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}\right) + t\right) + s - s^2\right) \Phi.$$

This expression is equal to zero if and only if

$$t = \frac{1}{2}(s^2 - s) - \frac{1}{m} \left(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}\right),$$

which is equivalent with $Q = N(s)$. \square

Remarks 1) If $a_1 = a_2$, $c_1 = c_2$, then the proof of Proposition 3.1 shows that all “automorphs” of an MT-matrix are of the form $e^{\frac{R}{6}s}$ for some integer s .

2) All integral “isomorphs” are actually contained in a proper congruence subgroup of $SL(3, \mathbb{Z})$, namely the matrices which are orthogonal modulo 3.

3) Notice that due to cancellation the matrix $N(s)$ can be written more compactly as follows,

$$N(s) = \frac{1}{m^2}\Gamma_0 + \Gamma_2 + \frac{s}{m}(\Omega_0 + m\Omega_1) + \frac{s^2 - s}{2}\Phi^t.$$

4 Markoff triples and quadratic residues

The point of departure in this section is the following matrix identity within the settings of section 3. Let

$$W = W(a_i, b_i, c_i) = \begin{pmatrix} c_i & 0 & 2a_i - mc_i \\ -b_i & 1 & c_i^2 - a_i^2 \\ a_i & 0 & ma_i - 2c_i \end{pmatrix}, i = 1, 2$$

then

(4.1)

$$\begin{aligned} N(0) &= W(a_2, b_2, c_2)W(a_1, b_1, c_1)^{-1} = \frac{1}{2m^2}W(a_2, b_2, c_2)W(a_1, b_1, c_1)^{\text{adj}} \\ &= \frac{1}{2m^2} \begin{pmatrix} c_2 & 0 & 2a_2 - mc_2 \\ -b_2 & 1 & c_2^2 - a_2^2 \\ a_2 & 0 & ma_2 - 2c_2 \end{pmatrix} \begin{pmatrix} ma_1 - 2c_1 & 0 & mc_1 - 2a_1 \\ 2mc_1 & 2m^2 & 2ma_1 \\ -a_1 & 0 & c_1 \end{pmatrix}. \end{aligned}$$

This identity separates the two Markoff triples with the property $m = a_1c_1 - b_1 = a_2c_2 - b_2$. For a single Markoff triple (a, b, c) the matrix $W(a, b, c)$ in turn gives rise to the following identity

(4.2)

$$W(a, b, c)^t M(a, b, c) W(a, b, c) = \begin{pmatrix} 0 & m & 0 \\ m & 1 & m^2 \\ 0 & -m^2 & -4m^2 \end{pmatrix}.$$

Significantly, the matrix on the right hand side depends on m only. Also notice that an application of the matrix R to the second column of W yields the third

column, while an application of R to the third column of W yields $4m$ times the first column of W . The following identity exhibits the intrinsic symmetry of this matrix,

$$W(c, b, a) = \mathcal{J}W(a, b, c) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

To get a better understanding of the architecture of the matrix on the right hand side of (4.2) we observe first that

$$\begin{pmatrix} 0 & m & 0 \\ m & 1 & m^2 \\ 0 & -m^2 & -4m^2 \end{pmatrix} = \begin{pmatrix} 0 & m & 0 \\ m & 1 & m^2 \\ 0 & m^2 & 4m^2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Both of these factors are associated with the nilpotent matrix on the right hand side of the conjugation

$$W(a, b, c)^{-1} R(a, b, c) W(a, b, c) = \begin{pmatrix} 0 & 0 & 4m \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

as follows: The first factor, which is self-adjoint, conjugates the matrix $\begin{pmatrix} 0 & 0 & 4m \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

to its adjoint $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 4m & 0 & 0 \end{pmatrix}$, while the second factor, which is a self-adjoint

involution, conjugates $\begin{pmatrix} 0 & 0 & 4m \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ to $-\begin{pmatrix} 0 & 0 & 4m \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Any matrix Y of

this design has the following “automorph” property,

$$\exp\left(s \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 4m & 0 & 0 \end{pmatrix}\right) Y \exp\left(-s \begin{pmatrix} 0 & 0 & 4m \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\right) = Y,$$

where $\exp(\cdot)$ denotes the exponential function, and s is a rational number. This construction works essentially for any nilpotent 3×3 matrix. Conversely, any matrix Y with the indicated “automorph” property must have the form

$$Y = \begin{pmatrix} 0 & \alpha & 0 \\ \alpha & \gamma & \beta \\ 0 & -\beta & -2m\alpha \end{pmatrix},$$

for arbitrary values α, β and γ . In the context of (1.2) we have $\alpha = m, \beta = m^2$ and $\gamma = 1$.

Remark The following observation, which will not be used in the sequel, is of some interest. Let

$$\mathcal{U} = W \begin{pmatrix} 1 & 0 & 0 \\ -m & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} c & 0 & 2a - mc \\ -ac & 1 & c^2 - a^2 \\ a & 0 & ma - 2c \end{pmatrix},$$

and let

$$\mathcal{Q} = \begin{pmatrix} 1 & \frac{a}{2} & \frac{b}{2} \\ \frac{a}{2} & 1 & \frac{c}{2} \\ \frac{b}{2} & \frac{c}{2} & 1 \end{pmatrix} = \frac{1}{2}(M(a, b, c) + M(a, b, c)^t)$$

Then

$$\mathcal{U}^t \mathcal{Q} \mathcal{U} = \begin{pmatrix} -m^2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -4m^2 \end{pmatrix}.$$

This identity shows that the column vectors of the matrix \mathcal{U} form an orthogonal basis with respect to the (indefinite) ternary quadratic form determined by the symmetric matrix \mathcal{Q} , which has a determinant equal to 1 if and only if (a, b, c) is a Markoff triple.

We are now going to state a property that exhibits the intrinsic rigidity of the identity (4.2).

4.1 Proposition For any four positive integers a, b, c, q , the following two conditions are equivalent

- a) The triple (a, b, c) is Markoff, and $q = ac - b$.
- b) There exists an integral 3x3 matrix $W = (w_{ij})$ with the properties

$$W^t M(a, b, c) W = \begin{pmatrix} 0 & q & 0 \\ q & 1 & q^2 \\ 0 & -q^2 & -4q^2 \end{pmatrix},$$

and $w_{12} = w_{32} = 0, w_{22} = 1$.

Proof By (4.2), a) implies b). To show that b) implies a), we first observe that

$$\det \begin{pmatrix} 0 & m & 0 \\ m & 1 & m^2 \\ 0 & -m^2 & -4m^2 \end{pmatrix} = 4m^4, \text{ and therefore } \det(W) = \pm 2m^2. \text{ We choose}$$

W to have a positive determinant. Letting $X = (x_{ij}) = W^{\text{adj}}$, we can restate

the matrix identity in b),

$$\begin{pmatrix} x_{11} & x_{21} & x_{31} \\ 0 & 2m^2 & 0 \\ x_{13} & x_{23} & x_{33} \end{pmatrix} \begin{pmatrix} 0 & m & 0 \\ m & 1 & m^2 \\ 0 & -m^2 & -4m^2 \end{pmatrix} \begin{pmatrix} x_{11} & 0 & x_{13} \\ x_{21} & 2m^2 & x_{23} \\ x_{31} & 0 & x_{33} \end{pmatrix} = 4m^4 \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Reading off the identities for those entries only which are located on or below the diagonal, with the exception of entry (2,2) which is trivial, yields,

$$\text{Entry (1,1): } 2mx_{11}x_{21} + x_{21}^2 - 4m^2x_{31}^2 = 4m^4$$

$$\text{Entry (2,1): } mx_{11} + x_{21} + m^2x_{31} = 0$$

$$\text{Entry (3,1): } mx_{11}x_{23} + mx_{13}x_{21} + x_{21}x_{23} - m^2x_{21}x_{33} + m^2x_{23}x_{31} - 4m^2x_{31}x_{33} = 0$$

$$\text{Entry (3,2): } mx_{13} + x_{23} - m^2x_{33} = 0$$

$$\text{Entry (3,3): } 2mx_{13}x_{23} + x_{23}^2 - 4m^2x_{33}^2 = 4m^4.$$

Combining the identities from entries (1,1) and (2,1) yields

(4.3)

$$x_{21}^2 + 2mx_{21}x_{31} + 4m^2x_{31}^2 + 4m^4 = 0 \quad .$$

Combining the identities from entries (3,2) and (3,3) yields

(4.4)

$$x_{23}^2 - 2m^2x_{23}x_{33} + 4m^2x_{33}^2 + 4m^4 = 0.$$

Finally, substituting the identities from entries (2,1) and (3,2) into the identity for entry (3,1) yields

(4.5)

$$x_{21}x_{23} + 4m^2x_{31}x_{33} = 0.$$

It follows from (4.3) and (4.4), respectively, that x_{21} and x_{23} are divisible by $2m$. Thus, letting

$$x_{21}^* = \frac{x_{21}}{2m}, x_{23}^* = \frac{x_{23}}{2m},$$

we obtain

(4.3)*

$$(x_{21}^*)^2 + mx_{21}^*x_{31} + x_{31}^2 + m^2 = 0,$$

(4.4)*

$$(x_{23}^*)^2 - mx_{23}^*x_{33} + x_{33}^2 + m^2 = 0,$$

(4.5)*

$$x_{21}^*x_{23}^* + x_{31}x_{33} = 0.$$

It follows from (4.3)* through (4.5)* that

$$|x_{21}^*| = |x_{33}|, |x_{23}^*| = |x_{31}|, x_{21}^*x_{31} < 0.$$

These last four conditions show that, up to a minus sign, the matrix X has exactly the form of the adjugated matrix of W in (4.1). It is now straightforward to check that the numbers a, b, c, m have the properties claimed in a). \square

Remarks 1) More generally, the following can be shown.

There exists a matrix $X = (x^{(1)}, x^{(2)}, x^{(3)}) \in M_3(\mathbb{Z})$ solving the matrix equation

$$X^t M(a, b, c) X = \begin{pmatrix} 0 & q & 0 \\ q & 1 & q^2 \\ 0 & -q^2 & -4q^2 \end{pmatrix},$$

such that the vector $x^{(2)}$ has length 1, if and only if (a, b, c) is a Markoff triple. Moreover

$$\begin{aligned} q &= c \text{ if } x^{(2)} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \\ q &= 3ac - b \text{ if } x^{(2)} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \\ q &= a \text{ if } x^{(2)} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned}$$

2) It is quite natural to wonder to what degree the matrix on the right hand side of (4.2) is uniquely determined by the discussion so far. The answer is, not as much as one is led to suspect. As a matter of fact, essentially everything that has been said so far works with minor adjustments just as well if the matrix $W = W(a, b, c)$ is being replaced by

$$Z^{\text{adj}} = \begin{pmatrix} -2c & 2a - mc & mc \\ 2ac & c^2 - a^2 & -mb \\ -2a & ma - 2c & ma \end{pmatrix},$$

where

$$Z = Z(a, b, c) = \begin{pmatrix} c & m & a \\ -a & 0 & c \\ a & 2 & c \end{pmatrix},$$

satisfying $\det(Z) = 2m^2$. All one has to do is to replace the second condition in Proposition 4.1 part b) by the following,

$$z_{12} = m, z_{22} = 0, z_{32} = 2.$$

The identity taking the place of (4.2) then becomes

(4.6)

$$(Z^{\text{adj}})^t M(a, b, c) Z^{\text{adj}} = \begin{pmatrix} -4m^2 & 2m^3 & 2m^3 \\ -2m^3 & -4m^2 & 0 \\ 2m^3 & 0 & 0 \end{pmatrix} = 2m^2 \begin{pmatrix} -2 & m & m \\ -m & -2 & 0 \\ m & 0 & 0 \end{pmatrix}.$$

One also has the identity,

$$ZW = \begin{pmatrix} 0 & m & 0 \\ 0 & 0 & 2m^2 \\ 2m & 2 & 0 \end{pmatrix}.$$

In a way the matrix W is related to the nilpotent matrix R , while the matrix Z is related to R^t . In fact, R^t applied to the last column vector of Z^t yields four times the second column vector of Z^t , while an application of R^t to the second column vector of Z^t yields $2m$ times the first row vector of Z^t . As we shall see shortly, however, the relationship between these two matrices is more intimate than appears to be the case at first sight.

The next step is to consider the general diophantine matrix equation

(4.7)

$$X^t M(a, b, c) X = \begin{pmatrix} 0 & q & 0 \\ q & 1 & q^2 \\ 0 & -q^2 & -4q^2 \end{pmatrix}; X \in \mathbf{M}_3(\mathbb{Z}), q \in \mathbb{N}; \det(X) > 0,$$

where (a, b, c) is a Markoff triple. We shall see shortly that, after imposing a slightly technical restriction, this equation has a solution if and only if q is divisible by 3 and -1 is a quadratic residue modulo $\frac{q}{3}$. Before we go into that we give a brief summary of some pertinent number theoretic facts, which can be readily gleaned from the standard literature (see [L], for part a) and b); [Pn], Satz 2.4, or more generally, [M1], [Ni] for part c)).

4.2 Lemma a) For any integer n there exists an element ε in the residue class ring \mathbb{Z}_n , such that $\varepsilon^2 = -1$ (in other words, -1 is a quadratic residue modulo n) if and only any odd prime factor p of n has the property $p \equiv 1 \pmod{4}$.

b) If n is an integer which is not divisible by 4 such that -1 is a quadratic residue modulo n , and l is the number of distinct odd prime factors dividing n , then there are exactly 2^l elements in \mathbb{Z}_n whose square is equal to -1 .

c) For any solution of the diophantine equation $k^2 + 1 = nl; n, l > 0$, there exists a matrix

$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{Sl}(2, \mathbb{Z})$ with such that

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}^t = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} n & k \\ k & l \end{pmatrix}.$$

If $k \geq 0$, then there exists a unique matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{Sl}(2, \mathbb{Z})$ with non-negative entries having this property.

If (a, b, c) is a Markoff triple, we let $\mathfrak{m} = \frac{ac-b}{3}$ if $ac-b$ is odd, and $\mathfrak{m} = \frac{ac-b}{6}$ if $ac-b$ is even. Since $a^2 + c^2 = 0$ modulo \mathfrak{m} , we have $\alpha^2 = -1$, where α is the element in $\mathbb{Z}_{\mathfrak{m}}$ corresponding to $\frac{a}{c}$.

We are now going to tackle the system (4.7). First we take the transposed matrices on both sides of (4.7) and subtract the result from (4.7), yielding

$$(4.8) \quad X^t \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix} X = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 2q^2 \\ 0 & -2q^2 & 0 \end{pmatrix}.$$

The matrix in the middle on the left hand side has rank 2, and the vector $(c, -b, a)^t$ is in the kernel of this matrix. Writing

$$X = (x^{(1)}, x^{(2)}, x^{(3)}),$$

we infer from (4.8) that

$$(x^{(1)})^t \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix} x^{(i)} = 0, \text{ for } i = 1, 2, 3.$$

Since X is invertible, its column vectors are linearly independent, and this entails

$$(x^{(1)})^t \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix} = 0,$$

which in turn implies that $x^{(1)}$ and $(c, -b, a)^t$ are linearly dependent. We now impose the technical restriction mentioned above.

$$(4.9) \quad (x^{(1)})^t = (c, -b, a)^t.$$

Under this assumption, we are first going to deal with the Markoff triple (3,3,3). In other words, we want to solve the system

(4.10)

$$\begin{pmatrix} x_{11} & x_{21} & x_{31} \\ x_{12} & x_{22} & x_{32} \\ x_{13} & x_{23} & x_{33} \end{pmatrix} \begin{pmatrix} 1 & 3 & 3 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix} = \\
\begin{pmatrix} x_{11}^2 + 3x_{11}x_{21} + x_{21}^2 & x_{11}x_{12} + 3x_{11}x_{22} + x_{21}x_{22} & x_{11}x_{13} + 3x_{11}x_{23} + x_{21}x_{23} \\ +3x_{11}x_{31} + 3x_{21}x_{31} + x_{31}^2 & +3x_{11}x_{32} + 3x_{21}x_{32} + x_{31}x_{32} & +3x_{11}x_{33} + 3x_{21}x_{33} + x_{31}x_{33} \\ x_{11}x_{12} + 3x_{12}x_{21} + x_{21}x_{22} & x_{12}^2 + 3x_{12}x_{22} + x_{22}^2 & x_{12}x_{13} + 3x_{12}x_{23} + x_{22}x_{23} \\ +3x_{12}x_{31} + 3x_{22}x_{31} + x_{31}x_{32} & +3x_{12}x_{32} + 3x_{22}x_{32} + x_{32}^2 & +3x_{12}x_{33} + 3x_{22}x_{33} + x_{32}x_{33} \\ x_{11}x_{13} + 3x_{13}x_{21} + x_{21}x_{23} & x_{12}x_{13} + 3x_{13}x_{22} + x_{22}x_{23} & x_{13}^2 + 3x_{13}x_{23} + x_{23}^2 \\ +3x_{13}x_{31} + 3x_{23}x_{31} + x_{31}x_{33} & +3x_{13}x_{32} + 3x_{23}x_{32} + x_{32}x_{33} & +3x_{13}x_{33} + 3x_{23}x_{33} + x_{33}^2 \end{pmatrix} \\
= \begin{pmatrix} 0 & q & 0 \\ q & 1 & q^2 \\ 0 & -q^2 & -4q^2 \end{pmatrix},
\end{pmatrix}$$

where at this point we shall assume that q is an odd integer divisible by 3. By assumption we have,

(4.11)

$$x_{11} = x_{31} = -x_{21} = 3.$$

The entry (1,2) or (2,1) yields,

(4.12)

$$x_{12} + 2x_{22} + x_{32} = \frac{q}{3}.$$

The entry (1,3) or (3,1) yields,

(4.13)

$$x_{13} + 2x_{23} + x_{33} = 0.$$

While entry (3,3) yields only $x_{23} + x_{33} = \pm 2q$, subtracting entry (3,2) from entry (2,3) yields,

(4.14)

$$x_{23} + x_{33} = 2q.$$

Combination of (4.12) with entry (2,2) yields,

(4.15)

$$\left(\frac{q}{3}\right)^2 + \frac{q}{3}(x_{32} - x_{22}) - (x_{32} + x_{22})^2 = 1$$

Finally, combining (4.12), (4.14) and entry (2,3) yields,

(4.16)

$$x_{33} - 6(x_{32} + x_{22}) = q.$$

Up to this point we have only extracted necessary conditions for the solvability of (4.9) and (4.10). We turn now to their sufficiency.

Letting

$$(4.17) \quad \alpha = x_{23}, \beta = x_{33}, \gamma = x_{32} - x_{22}, \varepsilon = x_{32} + x_{22},$$

we can recast the above identities as follows. Instead of (4.14) we write

$$(4.18) \quad \alpha + \beta = 2q.$$

Instead of (4.15) we write

$$(4.19) \quad \left(\frac{q}{3}\right)\left(\frac{q}{3} + \gamma\right) - \varepsilon^2 = 1.$$

Instead of (4.16) we write

$$(4.20) \quad \beta = 6\varepsilon + q.$$

The identity (4.19) is telling us that

$$\varepsilon^2 = -1 \text{ modulo } \frac{q}{3}.$$

So if we let ε be any number with this property

$$(4.21) \quad \varepsilon^2 = -1 + \frac{q}{3}j,$$

and if we let

$$\gamma = j - \frac{q}{3}, \beta = 6\varepsilon + q, \alpha = 2q - \beta,$$

then we can use (4.12) and the last two identities in (4.17) to solve for all three entries in the second column of the matrix X . Note that, since by our assumption q is an odd integer, (4.19) shows that ε is odd (even) if and only if γ is odd (even). This ensures that by virtue of the last two identities in (4.17) the numbers x_{22} and x_{32} are integers. Hence, x_{12} is an integer as well. By (4.13), (4.18) and (4.20) we can now solve for the three entries in the last column of the matrix X in terms of ε and j as well, all numbers being integers. To summarize, we have shown that all integral solutions of the system (4.9) and (4.10) have the form

$$X = \begin{pmatrix} 3 & \frac{q}{6} - \frac{3\varepsilon}{2} + \frac{j}{2} & -3q + 6\varepsilon \\ -3 & \frac{1}{2}(\varepsilon - j + \frac{q}{3}) & q - 6\varepsilon \\ 3 & \frac{1}{2}(\varepsilon + j + \frac{q}{3}) & q + 6\varepsilon \end{pmatrix},$$

provided q is an odd integer which is divisible by 3, and the integers ε and j solve the diophantine equation $\varepsilon^2 = -1 + \frac{q}{3}j$. In order to see that the same conclusion holds for even integers q as well, we observe that if q is even, then ε has to be

odd. But this means that $\varepsilon^2 + 1 = 4n + 2$ for some integer n , and therefore j has to be odd as well. So it follows that all three entries in the second column of the matrix X are integers in case q is even. In conclusion, what we have shown is the first part of the following statement.

4.3 Proposition a) The system (4.9) and (4.10) has an integral solution X if and only if -1 is a quadratic residue modulo the integer $\frac{q}{3}$.

b) The integral solutions of (4.9) and (4.10) are completely parametrized by all the square roots of -1 in the residue class ring associated with $\frac{q}{3}$ in the following sense: Given two pairs of numbers, (ε_1, j_1) and (ε_2, j_2) satisfying (4.21), such that $\varepsilon_1 = \varepsilon_2$ modulo $\frac{q}{3}$, each giving rise to the solutions X_1 and X_2 of (4.9) and (4.10), respectively, there exists an integer i such that

$$e^{\frac{i}{2}\mathbf{R}}X_1 = X_2,$$

where

$$\mathbf{R} = \begin{pmatrix} -3 & -4 & -1 \\ 1 & 0 & -1 \\ 1 & 4 & 3 \end{pmatrix}.$$

The proof of the second part of this proposition will be given below where we deal with general Markoff triples.

Remark It follows from (4.16), (4.14) and (4.13) that all entries in the last column of X are divisible by 3.

The following corollary, which is of some independent interest, will not be used in the sequel.

4.4 Corollary If X is an integral solution of (4.9) and (4.10), and

$$X^* = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} X \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

then

$$e^{(E - \frac{\beta}{2q}\mathbf{R})}X = X^*.$$

4.5 Corollary a) For any Markoff triple the system (4.7) and (4.9) has an integral solution X if and only if -1 is a quadratic residue modulo the integer $\frac{q}{3}$.

b) The integral solutions of (4.7) and (4.9) are completely parametrized by all the square roots of -1 in the residue class ring associated with $\frac{q}{3}$ in the following sense: Given two pairs of numbers, (ε_1, j_1) and (ε_2, j_2) satisfying (4.21), such that $\varepsilon_1 = \varepsilon_2$ modulo $\frac{q}{3}$, each giving rise to the solutions X_1 and X_2 of (4.7) and (4.9), respectively, there exists an integer i such that

$$e^{\frac{i}{2}\mathbf{R}}X_1 = X_2,$$

where

$$\mathbf{R} = \frac{1}{3} \begin{pmatrix} a^2 + b^2 - abc & 2a + bc - ac^2 & 2b - ac \\ bc - 2a & c^2 - a^2 & 2c - ab \\ ac - 2b & -2c - ab + a^2c & abc - b^2 - c^2 \end{pmatrix}.$$

Proof By Proposition 1.2 a) any integral solution of the system (4.7) for the Markoff triple (3,3,3) can be transformed into an integral solution of the system (4.7) for an arbitrary Markoff triple, and vice versa. The first identity in Proposition 1.2 b) ensures that property (4.9) is preserved under such a transformation. \square

Our next task is to characterize the solutions of the system (4.7) and (4.9), whose existence has been established in Proposition 4.5, for arbitrary Markoff triples more specifically.

4.6 Proposition Suppose that $\frac{q}{3}$ is an integer such that -1 is a quadratic residue modulo the integer $\frac{q}{3}$. Then given an integral solution X of the system (4.7) and (4.9), there exist two integers ε and j such that $\varepsilon^2 + 1 = \frac{q}{3}j$, and there exist three integers α, k, l , such that $c\alpha - a = mk$ and $\alpha^2 + 1 = \frac{m}{3}l$, having the following property,

(4.22)

$$ZX = Q = \mathcal{A}\mathcal{B},$$

where

$$Z = \begin{pmatrix} c & m & a \\ -a & 0 & c \\ a & 2 & c \end{pmatrix}, Q = \begin{pmatrix} 0 & q & 0 \\ 0 & m\varepsilon - q\alpha & 2mq \\ 2m & \frac{1}{3}(ql + mj) - 2\alpha\varepsilon & 4(m\varepsilon - q\alpha) \end{pmatrix}$$

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & 0 \\ -\alpha & m & 0 \\ \frac{l}{3} & -2\alpha & m \end{pmatrix}, \mathcal{B} = \begin{pmatrix} 0 & q & 0 \\ 0 & \varepsilon & 2q \\ 2 & \frac{j}{3} & 4\varepsilon \end{pmatrix}.$$

Conversely, any integral solution of the form (4.22) is also a solution of the system (4.7) and (4.9).

Remarks 1) Notice the separation of data pertaining to the quadratic residues for the numbers m and q , respectively, which results from the factorization of the matrix Q into \mathcal{A} and \mathcal{B} .

2) If (a, b, c) is an arbitrary triple of positive integers admitting a solution that can be factored as in (4.22), then (a, b, c) is a Markoff triple. This is a consequence of the identity

$$X^t \begin{pmatrix} c \\ m \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ q \\ 0 \end{pmatrix},$$

as well as the observation that the first entry in this vector identity is equivalent to the Markoff property.

3) Denoting the i -th column vector of the matrix X in (4.22) by $x^{(i)}$, the following two identities hold

$$R(a, b, c)x^{(2)} = x^{(3)}, R(a, b, c)x^{(3)} = 4qx^{(1)}.$$

Before we turn to the proof of Proposition 4.6 we state some consequences and identities. We call two solutions X_1 and X_2 of the system (4.7) and (4.9) equivalent if and only if

$$e^{\frac{i}{2}\mathbf{R}}X_1 = X_2, \text{ where } \mathbf{R} = \frac{1}{3} \begin{pmatrix} -c^2 & 2a - cm & 2b - ac \\ bc - 2a & c^2 - a^2 & 2c - ab \\ ac - 2b & am - 2c & a^2 \end{pmatrix},$$

for some integer i . The following restates part b) of Proposition 4.3 and Part b) of Corollary 4.5.

4.7 Corollary Two solutions of the system (4.7) and (4.9) are equivalent if and only if they are associated with two numbers ε_1 and ε_2 which are equal modulo $\frac{q}{3}$. In particular the number of inequivalent integral solutions of the system (4.7) and (4.9) is the same for all Markoff triples.

Proof First we observe that for $R = 3\mathbf{R}$

$$R(Z^{-1}\mathcal{A}\mathcal{B}) = (Z^{-1}\mathcal{A}\mathcal{B}) \begin{pmatrix} 0 & 0 & 4q \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

This follows from the following sequence of basic identities.

$$RZ^{-1} = Z^{-1} \begin{pmatrix} 0 & 0 & 0 \\ 2m & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 \\ m & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \mathcal{A} = \mathcal{A} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \mathcal{B} = \frac{1}{2} \mathcal{B} \begin{pmatrix} 0 & 0 & 4q \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Next we observe, writing temporarily $\mathcal{B} = \mathcal{B}_\varepsilon$,

$$\mathcal{B}_\varepsilon \exp\left(\frac{x}{2} \begin{pmatrix} 0 & 0 & 4q \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\right) = \mathcal{B}_{\varepsilon+xq},$$

where $\exp(x) = e^x$. Putting all this together, yields

$$\exp\left(\frac{1}{2}x\mathbf{R}\right)(Z^{-1}\mathcal{A}\mathcal{B}_\varepsilon) = Z^{-1}\mathcal{A}\mathcal{B}_{\varepsilon+x\frac{q}{3}},$$

from which the claim follows. \square

4.8 Corollary Given any integers α, l , such that $\alpha^2 + 1 = ml$ the following identities hold.

(4.23)

$$(Z^{-1}\mathcal{A})^t M(a, b, c)(Z^{-1}\mathcal{A}) = \frac{1}{2} \begin{pmatrix} 0 & 1 & 1 \\ -1 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Moreover, the numbers α, k, l can be chosen such that

(4.24)

$$\mathcal{A}^{-1}Z\epsilon\frac{1}{3}\mathbf{M}_3(\mathbb{Z}) \text{ if } m \text{ is odd, } \mathcal{A}^{-1}Z\epsilon\frac{1}{6}\mathbf{M}_3(\mathbb{Z}) \text{ if } m \text{ is even.}$$

Proof The identity (4.23) follows from the identity (4.6), as well as the identity

(4.25)

$$\mathcal{A}^t \begin{pmatrix} -2 & m & m \\ -m & -2 & 0 \\ m & 0 & 0 \end{pmatrix} \mathcal{A} = m^2 \begin{pmatrix} 0 & 1 & 1 \\ -1 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

In order to show the validity of (4.24) we choose q in Proposition 4.6 such that $\frac{q}{3} = 1$ modulo 4 and $\frac{q}{3}$ is a prime number which does not divide m . Then, by (4.22),

$$\mathcal{A}^{-1}Z = \frac{1}{\det(\mathcal{A})}\mathcal{A}^{\text{adj}}Z = \frac{1}{m^2}\mathcal{A}^{\text{adj}}Z = \frac{1}{2q^2}\mathcal{B}X^{\text{adj}} = \frac{1}{\det(X)}\mathcal{B}X^{\text{adj}} = \mathcal{B}X^{-1}.$$

Since $\frac{q}{3}$ does not divide $\frac{m}{3}$ by assumption, it follows that none of the reduced fractions in the entries of the matrix $\mathcal{A}^{-1}Z$ is divisible by a prime factor of m distinct from 2 or 3. Furthermore, choosing α and k as in Proposition 4.6,

$$c\alpha - a = mk ,$$

which, by virtue of the Markoff property implies that there exists an integer k^* such that

$$a\alpha + c = mk^* ,$$

we obtain

$$\begin{aligned} \mathcal{A}^{-1}Z &= \frac{1}{m^2} \begin{pmatrix} m^2 & 0 & 0 \\ \alpha m & m & 0 \\ \frac{ml}{3} - 2 & 2\alpha & m \end{pmatrix} \begin{pmatrix} c & m & a \\ -a & 0 & c \\ a & 2 & c \end{pmatrix} = \\ &= \frac{1}{m^2} \begin{pmatrix} m^2c & m^3 & am^2 \\ m(c\alpha - a) & \alpha m^2 & m(a\alpha + c) \\ m(\frac{cl}{3} + a) - 2(a\alpha + c) & \frac{m^2l}{3} & m(\frac{al}{3} + c) + 2(c\alpha - a) \end{pmatrix} = \\ &= \frac{1}{m} \begin{pmatrix} mc & m^2 & am \\ c\alpha - a & \alpha m & a\alpha + c \\ \frac{cl}{3} + a - 2k^* & \frac{ml}{3} & \frac{al}{3} + c + 2k \end{pmatrix} , \end{aligned}$$

and so the denominators of the reduced fractions in the entries of $\mathcal{A}^{-1}Z$ divide 3 if m is odd, and they divide 6 if m is even. \square

Remark Swapping the roles of the matrices W and Z and, accordingly \mathcal{A} and \mathcal{B} , one can obtain an identity akin to (4.23). Combining (4.2) with the identity,

$$(4.26) \quad (\mathcal{B}^{-1})^t \begin{pmatrix} 0 & q & 0 \\ q & 1 & q^2 \\ 0 & -q^2 & -4q^2 \end{pmatrix} \mathcal{B}^{-1} = \frac{1}{2} \begin{pmatrix} 0 & 1 & 1 \\ -1 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix} ,$$

for $q = m$ leads to

$$(4.27) \quad (W\mathcal{B}^{-1})^t M(a, b, c) (W\mathcal{B}^{-1}) = \frac{1}{2} \begin{pmatrix} 0 & 1 & 1 \\ -1 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix} .$$

The following two identities shed some more light on the nature of the matrices \mathcal{A} and \mathcal{B} .

4.9 Lemma If $\alpha_i, l_i, i = 1, 2$ are two sets of data as in Proposition 4.6, and $\mathcal{A}_i, \mathcal{B}_i$ are the corresponding matrices associated with them, then

(4.28)

$$\mathcal{A}_1^{-1}\mathcal{A}_2 = \exp\left(\left(\frac{\alpha_1 - \alpha_2}{m}\right)\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}\right), \mathcal{A}_2\mathcal{A}_1^{-1} = \exp\left(\left(\frac{\alpha_1 - \alpha_2}{m}\right)\begin{pmatrix} 0 & 0 & 0 \\ m & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}\right),$$

(4.29)

$$\mathcal{B}_2\mathcal{B}_1^{-1} = \exp\left(\left(\frac{\varepsilon_2 - \varepsilon_1}{q}\right)\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}\right), \mathcal{B}_1^{-1}\mathcal{B}_2 = \exp\left(\left(\frac{\varepsilon_2 - \varepsilon_1}{q}\right)\begin{pmatrix} 0 & 0 & 4q \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\right).$$

The proof of Lemma 4.7 is obtained through straightforward manipulations.

Proof of Proposition 4.6 That any matrix X having the properties stipulated in (4.22) is a solution of the sytem (4.7) and (4.9) can be seen through an application of (4.6), (4.25) and (4.26). In order to show that any integral solution of (4.7) and (4.9) has the claimed form, we are going to proceed as in the line of reasoning leading up to Proposition 4.3. This means that we need to solve the system (4.7) and (4.9) in such a way as to exhibit the dependence of the solutions on the data pertaining to the corresponding quadratic residues. Extending (4.10) to the case of a general Markoff triple we consider,

(4.30)

$$\begin{pmatrix} x_{11} & x_{21} & x_{31} \\ x_{12} & x_{22} & x_{32} \\ x_{13} & x_{23} & x_{33} \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix} =$$

$$\begin{pmatrix} x_{11}^2 + ax_{11}x_{21} + x_{21}^2 & x_{11}x_{12} + ax_{11}x_{22} + x_{21}x_{22} & x_{11}x_{13} + ax_{11}x_{23} + x_{21}x_{23} \\ +bx_{11}x_{31} + cx_{21}x_{31} + x_{31}^2 & +bx_{11}x_{32} + cx_{21}x_{32} + x_{31}x_{32} & +bx_{11}x_{33} + cx_{21}x_{33} + x_{31}x_{33} \\ x_{11}x_{12} + ax_{12}x_{21} + x_{21}x_{22} & x_{12}^2 + ax_{12}x_{22} + x_{22}^2 & x_{12}x_{13} + ax_{12}x_{23} + x_{22}x_{23} \\ +bx_{12}x_{31} + cx_{22}x_{31} + x_{31}x_{32} & +bx_{12}x_{32} + cx_{22}x_{32} + x_{32}^2 & +bx_{12}x_{33} + cx_{22}x_{33} + x_{32}x_{33} \\ x_{11}x_{13} + ax_{13}x_{21} + x_{21}x_{23} & x_{12}x_{13} + ax_{13}x_{22} + x_{22}x_{23} & x_{13}^2 + ax_{13}x_{23} + x_{23}^2 \\ +bx_{13}x_{31} + cx_{23}x_{31} + x_{31}x_{33} & +bx_{13}x_{32} + cx_{23}x_{32} + x_{32}x_{33} & +bx_{13}x_{33} + cx_{23}x_{33} + x_{33}^2 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & q & 0 \\ q & 1 & q^2 \\ 0 & -q^2 & -4q^2 \end{pmatrix}.$$

By (4.9) we have

(4.31)

$$x_{11} = c, x_{21} = -b, x_{31} = a.$$

Entry (1,2) yields

(4.32)

$$cx_{12} + mx_{22} + ax_{32} = q.$$

Entry (1,3) yields

(4.33)

$$cx_{13} + mx_{23} + ax_{33} = 0.$$

Multiplying the (3,3) entries by m^2 and eliminating x_{23} yields $cx_{33} - ax_{13} = \pm 2mq$. In order to determine the proper sign we multiply the (2,3) entries by m^2 , eliminate x_{23} by means of (4.33), then we proceed in exactly the same fashion with the (3,2) entries, and obtain after subtracting the latter from the former,

(4.34)

$$cx_{33} - ax_{13} = 2mq.$$

Multiplying the (2,2) entries by m^2 and combining the result with (4.32) yields,

(4.35)

$$(ax_{12} - cx_{32})^2 - (ax_{12} + 2x_{22} + cx_{32})mq = -m^2 - q^2.$$

We consider the following factorization,

(4.36)

$$m = pd, q = pe; d, e \text{ and } p \text{ pairwise relatively prime.}$$

Then (4.35) implies that $ax_{12} - cx_{32}$ is divisible by p . Since d and e relatively prime, there exist integers ε_0 and α_0 such that

$$e\alpha_0 - d\varepsilon_0 = \frac{ax_{12} - cx_{32}}{p}.$$

or

(4.37)

$$q\alpha_0 - m\varepsilon_0 = ax_{12} - cx_{32}$$

Combining (4.35) and (4.37) yields

(4.38)

$$m^2(\varepsilon_0^2 + 1) + q^2(\alpha_0^2 + 1) = (ax_{12} + 2x_{22} + cx_{32} + 2\varepsilon_0\alpha_0)mq.$$

It follows from this that there exist integers j_0 and k_0 such that

(4.39)

$$\varepsilon_0^2 + 1 = ej_0, \alpha_0^2 + 1 = dk_0.$$

Now (4.37) implies

(4.40)

$$\alpha_0 = \frac{1}{q}(ax_{12} - cx_{32}) \text{ modulo } d,$$

while (4.32) implies

(4.41)

$$x_{32} = \frac{1}{a}(q - cx_{12}) \text{ modulo } d.$$

Combining (4.40) and (4.41) we obtain by virtue of the Markoff property

$$\alpha_0 = \frac{1}{q}(ax_{12} - \frac{c}{a}(q - cx_{12})) = (a + \frac{c^2}{a})\frac{x_{12}}{q} - \frac{c}{a} = \frac{mb}{aq}x_{12} - \frac{c}{a} = -\frac{c}{a} \text{ modulo } d.$$

Hence,

$$a\alpha_0 + a = 0 \text{ modulo } d,$$

or, again by the Markoff property,

(4.42)

$$c\alpha_0 - a = 0 \text{ modulo } d.$$

Let α and k be integers such that

(4.43)

$$c\alpha - a = mk,$$

and let l be an integer such that

(4.44)

$$\alpha^2 + 1 = \frac{m}{3}l.$$

Now (4.42) and (4.43) imply that there exists an integer u such that

(4.45)

$$\alpha - \alpha_0 = du.$$

Let

(4.46)

$$\varepsilon = \varepsilon_0 + eu.$$

Then (4.37), (4.45) and (4.46) yield

$$\begin{aligned} q\alpha - m\varepsilon &= q\alpha - m\varepsilon_0 - pdeu = q\alpha - m\varepsilon_0 - qdu = q\alpha - m\varepsilon_0 - q(\alpha - \alpha_0) = q\alpha_0 - m\varepsilon_0 \\ &= ax_{12} - cx_{32}. \end{aligned}$$

In conclusion

(4.47)

$$q\alpha - m\varepsilon = ax_{12} - cx_{32}.$$

Moreover,

$$\varepsilon^2 + 1 = \varepsilon_0^2 + 2e\varepsilon_0u + e^2u^2 + 1 = e(j_0 + 2\varepsilon_0u + eu^2),$$

or, letting $j^* = j_0 + 2\varepsilon_0u + eu^2$,

(4.48)

$$\varepsilon^2 + 1 = ej^*.$$

Since (4.35) and (4.47) yield

$$m^2(\varepsilon^2 + 1) + q^2(\alpha^2 + 1) = (ax_{12} + 2x_{22} + cx_{32} + 2\varepsilon\alpha)mq,$$

we finally obtain by virtue of (4.44) and (4.48),

(4.49)

$$ax_{12} + 2x_{22} + cx_{32} = \frac{q}{3}l + dj^* - 2\alpha\varepsilon$$

Putting it all together, (4.32) provides the first, (4.47) the second, and (4.49) the third linear identity, respectively, of the following system

(4.50)

$$\begin{pmatrix} c & m & a \\ -a & 0 & c \\ a & 2 & c \end{pmatrix} \begin{pmatrix} x_{12} \\ x_{22} \\ x_{32} \end{pmatrix} = \begin{pmatrix} q \\ m\varepsilon - q\alpha \\ \frac{q}{3}l + dj^* - 2\alpha\varepsilon \end{pmatrix}$$

We turn now to the third column of the matrix X . We have found two linear identities already, namely (4.33) and (4.34). To determine the third, we multiply the (2,3) entries by m^2 , which simplifies to

$$(ax_{12} - cx_{32})(cx_{33} - ax_{13}) + (x_{23} + cx_{33})mq = m^2q^2.$$

Combining this with (4.34) yields

$$2(ax_{12} - cx_{32}) + (x_{23} + cx_{33}) = mq,$$

or by (4.47),

$$x_{23} + cx_{33} = mq + 2(m\varepsilon - q\alpha).$$

Multiplying this by 2 and subtracting (4.34) from it, yields

$$ax_{13} + 2x_{23} + cx_{33} = 4(m\varepsilon - q\alpha),$$

which is the missing third identity. Putting it all together again, we have

(4.51)

$$\begin{pmatrix} c & m & a \\ -a & 0 & c \\ a & 2 & c \end{pmatrix} \begin{pmatrix} x_{13} \\ x_{23} \\ x_{33} \end{pmatrix} = \begin{pmatrix} 0 \\ 2mq \\ 4(m\varepsilon - q\alpha) \end{pmatrix}.$$

Finally, Markoff's property ensures that (4.31) implies

(4.52)

$$\begin{pmatrix} c & m & a \\ -a & 0 & c \\ a & 2 & c \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \\ x_{31} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 2m \end{pmatrix}.$$

Next we shall first deal with a special case, namely the situation where the numbers $\frac{m}{3}$ and $\frac{q}{3}$ are relatively prime. In this case $p = 3$ and $d = \frac{m}{3}$, and so, letting $j = j^*$, (4.50) reads

$$\begin{pmatrix} c & m & a \\ -a & 0 & c \\ a & 2 & c \end{pmatrix} \begin{pmatrix} x_{12} \\ x_{22} \\ x_{32} \end{pmatrix} = \begin{pmatrix} q \\ m\varepsilon - q\alpha \\ \frac{1}{3}(ql + mj) - 2\alpha\varepsilon \end{pmatrix}.$$

This, combined with (4.51) and (4.52) yields the claimed identity $ZX = Q$, as well as the claimed factorization of Q into the matrices \mathcal{A} and \mathcal{B} , thus settling the claim in this particular case. In order to deal with the general case we observe that the combination of (4.50) through (4.52) yields the factorization

$$ZX = \mathcal{A} \begin{pmatrix} 0 & q & 0 \\ 0 & \varepsilon & 2q \\ 2 & \frac{j^*}{p} & 4\varepsilon \end{pmatrix}.$$

Solving for the second factor on the right hand side yields

(4.53)

$$\begin{pmatrix} 0 & q & 0 \\ 0 & \varepsilon & 2q \\ 2 & \frac{j^*}{p} & 4\varepsilon \end{pmatrix} = \mathcal{A}^{-1}ZX.$$

Next we are going to invoke (4.24) in Corollary 4.8, whose proof was based on the special case we have just settled. By the first statement in (4.24) the reduced fractions in the entries of the matrix $\mathcal{A}^{-1}Z$ are either integers or rational numbers whose denominator divides 6. Since X is integral, the same is true for the entries of the matrix $\mathcal{A}^{-1}ZX$ on the right hand side of (4.53). Since the denominator of the reduced fraction in the entry (3,2) of the matrix on the left hand side of (4.53) has exactly one factor 3, which, due to the fact that j^* as a product of prime factors which are either equal to 2 or equal to 1 modulo 4, does not cancel, that denominator can only be equal to 3 or 6. If at least one of the integers m or q is odd, then p has to be odd as well, in which case the said denominator is equal to 3. If both, m and q are even, then (4.47) implies that the integers ax_{12} and cx_{32} are both either odd or even. Since m , being a Markoff number, can have at most one even prime factor, and since this implies that d has to be odd, this together with (4.49) implies that j^* has to be even. In conclusion, the said denominator can not be 6, and therefore it has to be equal to 3. So, letting $j = \frac{3j^*}{p}$, our claim follows in the general case as well. \square

Remarks 1) Note that all the arguments in the proof of Proposition 4.6 are necessary for the existence of an integral solution of the system (4.7) and (4.9), they are not sufficient. Sufficiency rests entirely upon Corollary 4.5. However, since the factorization obtained in Proposition 4.6 is valid for all Markoff triples, in particular for the triple (3, 3, 3), the parametrization of the equivalence classes

of all integral solutions of the system (4.7) and (4.9) through quadratic residues of -1 is unique.

2) The case $m = q$ in Proposition 4.6 calls for some special attention. In this case we have the following particular form for the matrix product on the right hand side of (4.22),

$$\mathcal{AB} = \begin{pmatrix} 0 & m & 0 \\ 0 & m(\varepsilon - \alpha) & 2m^2 \\ 2m & (\varepsilon - \alpha)^2 + 2 & 4m(\varepsilon - \alpha) \end{pmatrix}.$$

Significantly, this matrix depends on m and the integer $\varepsilon - \alpha$ only. Since $\alpha^2 = -1, \varepsilon^2 = -1$ modulo m , it follows that there exists a factorization $\frac{m}{3} = pq$ if m is odd, $\frac{m}{6} = pq$ if m is even, with p and q being relatively prime integers. This observation reflects a rather general pattern. Given any integer n with a quadratic residue of -1 in the residue class ring \mathbb{Z}_n , and given a particular choice, k say, the differences $k - k^*$, where k^* ranges over all the other quadratic residues of -1 in \mathbb{Z}_n , correspond in a one-to-one way to all the factorizations of n divided by its even prime factors, into two relatively prime integers. Since all initial choices are equivalent in this regard, we can not hope to characterize a specific one, in our case α , and settle the uniqueness question within this framework. The characterization of α among all the other quadratic residues of -1 modulo $\frac{m}{3}$ is more implicit. It is expressed through the “almost” integrality of the matrix $\mathcal{A}^{-1}Z$ and its inverse. The first part of this statement was established in (4.24). Being of such an implicit nature however, this property is too elusive in order to lend itself for the establishment of the uniqueness of the set $\{\alpha, -\alpha\}$ modulo $\frac{m}{3}$, which is equivalent to the uniqueness claim of the Theorem. But as we shall see in Section 5, in addition to the generic encodings of differences of quadratic residues of -1 by means of relatively prime factorizations, there exists a one-to-one correspondence between all the quadratic residues of -1 modulo $\frac{m}{3}$ and all the factorizations of $\frac{m}{3}$ if m is odd, and $\frac{m}{6}$ if m is even, into two relatively prime integers, which is particular to Markoff numbers. It is this feature which will allow us to settle the uniqueness claim as enunciated in the Theorem.

2) The question arises of how much of the formalism in this section is particular to the setting of Markoff triples. In order to obtain a partial answer to this question we introduce the the following concept:

If $p \geq 3$ is an integer, then we call $(a, b, c) \in \mathbb{N}^3$ a p -triple if

(*)

$$a^2 + b^2 + c^2 = pabc + 3 - p.$$

The following statements hold true for p -triples:

(I) $(1, 1, 1)$ is a p -triple.

(II) If (a, b, c) is a p -triple then $(a, b, pac - b)$ and $(pac - b, a, c)$ are p -triples as well.

(III) Up to permutations of the components, any \mathfrak{p} -triple can be obtained through finitely many transitions as stipulated in (II).

(IV) All solutions of the diophantine matrix equation

$$X^t M(\mathfrak{p}\mathfrak{a}, \mathfrak{p}\mathfrak{b}, \mathfrak{p}\mathfrak{c}) X = \begin{pmatrix} 0 & \mathfrak{p}\mathfrak{q} & 0 \\ \mathfrak{p}\mathfrak{q} & 1 & \mathfrak{p}^2\mathfrak{q}^2 \\ 0 & -\mathfrak{p}^2\mathfrak{q}^2 & -4\mathfrak{p}^2\mathfrak{q}^2 \end{pmatrix}$$

for a given integer \mathfrak{q} for which -1 is a quadratic residue modulo \mathfrak{q} can be parametrized by the solutions of the equation $\varepsilon^2 = -1$ modulo \mathfrak{q} .

Properties (I) through (III) tell us that a tree of \mathfrak{p} -triples can be built in parallel to the developments in Section 1. Property (IV) is a reflection of the fact that Proposition 4.3a) and its proof carry over to the settings of \mathfrak{p} -triples.

The case $\mathfrak{p} = 3$ yields Markoff triples of course, and the factorization obtained in Proposition 4.6 is particular to this case. If we choose $\mathfrak{p} = 0$ in (*), then $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ is a solution of the equation if and only if $|\mathfrak{a}| = |\mathfrak{b}| = |\mathfrak{c}| = 1$. But if we choose $\mathfrak{p} = -1$, then we recover (essentially, i. e. up to a minus sign) the case of the Tchebycheff polynomials briefly discussed in Section 2.

5 Proof of the Theorem

Our first objective is to obtain a characterization of the equivalence classes of integers for which -1 is a quadratic residue modulo a Markoff number $\frac{m}{3} = \frac{ac-b}{3}$. Throughout we shall be using the following notation. Let $\mathfrak{m} = \frac{m}{3}$ if m is odd, and $\mathfrak{m} = \frac{m}{6}$ if m is even.

5.1 Lemma a) Let n be an integer such that $n^2 + 1 = \mathfrak{m}l$. Then there exists a (unique) factorization $\mathfrak{m} = pq$ into relatively prime factors such that

(5.1)

$$cn + a = pu, cn - a = qv; u, v \in \mathbb{Z}.$$

b) For any factorization $\mathfrak{m} = pq$ of \mathfrak{m} into relatively prime factors there is exactly one equivalence class of numbers n modulo \mathfrak{m} such that (5.1) holds.

Proof a) Since

$$(cn + a)(cn - a) = c^2n^2 - a^2 = c^2(\mathfrak{m}l - 1) - a^2 = c^2l\mathfrak{m} - (a^2 + c^2) = c^2l\mathfrak{m} - bm,$$

there exists a factorization $\mathfrak{m} = pq$ such that

$$\frac{cn + a}{p}, \frac{cn - a}{q} \in \mathbb{Z}.$$

Since both, p and q are relatively prime to ac as well as to n , the numbers p and q have to be relatively prime as well, and therefore they are also unique.

b) By Lemma 4.2 the number of equivalence classes of integers for which -1 is a quadratic residue modulo \mathfrak{m} , and the number of factorizations of \mathfrak{m} into two relatively prime factors, each factor being a product of odd primes only, is the same. Since part a) ensures already that we have an injective map from one set into the other, the claim follows. \square

We return now to the settings of the later part of Section 3, assuming the presence of two, at this point not necessarily distinct, Markoff triples with a common dominant member. In order to exploit the number theoretic features of the representation (3.4), we shall need the following sequence of lemmas, culminating with the factorization of m stated in Corollary 5.4 below.

5.2 Lemma If $q \neq 2, 3$ is a prime factor of m , then q does not divide at least one of the following two terms

$$a_1a_2 + c_1c_2, a_1a_2 - c_1c_2.$$

The same conclusion holds for the terms

$$a_1c_2 + c_1a_2, a_1c_2 - c_1a_2.$$

Proof Suppose the first statement were not true, i.e. both terms are divisible by q . Then q also divides

$$(a_1a_2 + c_1c_2) + (a_1a_2 - c_1c_2) = 2a_1a_2.$$

Since $q \neq 2, 3$, neither a_1 nor a_2 is divisible by q , and so this is impossible. The same argument proves the second statement. \square

5.3 Lemma If $q \neq 3$ is a prime factor of m , then

a) q divides $a_1c_2 - c_1a_2$ if and only if it divides $a_1a_2 + c_1c_2$,

b) q divides $a_1a_2 - c_1c_2$ if and only if it divides $a_1c_2 + c_1a_2$.

Proof a) If q divides $c_2 - c_1a_2$, then

$$a_1 = \frac{a_1}{a_2}a_2 \text{ and } c_1 = \frac{a_1}{a_2}c_2 \text{ modulo } q.$$

Hence

$$0 = mb_1 = a_1^2 + c_1^2 = \frac{a_1}{a_2}(a_1a_2 + c_1c_2) \text{ modulo } q,$$

which in turn implies

$$a_1a_2 + c_1c_2 = 0 \text{ modulo } q.$$

If, on the other hand, q divides $a_1a_2 + c_1c_2$, then

$$a_1 = \frac{a_1}{c_2}c_2 \text{ and } c_1 = -\frac{a_1}{c_2} \text{ modulo } q.$$

Hence

$$0 = mb_1 = a_1^2 + c_1^2 = \frac{a_1}{c_2}(a_1c_2 - c_1a_2) \text{ modulo } q,$$

which in turn implies

$$a_1c_2 - c_1a_2 = 0 \text{ modulo } q.$$

b) All one has to do is switch a_1 and c_1 , or equivalently, a_2 and c_2 , and copy the proof for part a). \square

5.4 Lemma Suppose that $m = nq^l$, $q \neq 2, 3$ is a prime factor, and n, q relatively prime. Then

$$\text{either } q^{2l} \text{ divides } a_1c_2 - c_1a_2 \text{ or } q^{2l} \text{ divides } a_1a_2 - c_1c_2.$$

Proof We shall need the following:

(5.2)

$$(a_1c_2 - c_1a_2)(a_1a_2 - c_1c_2) = m^2(b_1 - b_2)$$

To see this, we employ Markoff's property.

$$\begin{aligned} (a_1c_2 - c_1a_2)(a_1a_2 - c_1c_2) &= (a_1^2 + c_1^2)a_2c_2 - (a_2^2 + c_2^2)a_1c_1 = m(b_1a_2c_2 - b_2a_1c_1) = \\ m[(b_1 - a_1c_1)a_2c_2 - (b_2 - a_2c_2)a_1c_1] &= m^2(a_1c_1 - a_2c_2) = m^2[(a_1c_1 - b_1) - (a_2c_2 - b_2) + b_1 - b_2] = \\ m^2(b_1 - b_2). \end{aligned}$$

If $b_1 - b_2 = 0$, then the claim is obviously true, because one of the two terms is zero, while the other one and q are relatively prime. Now suppose that $b_1 - b_2 \neq 0$, and that q divides $a_1c_2 - c_1a_2$ and $a_1a_2 - c_1c_2$. Then by Lemma 5.3 q divides $a_1a_2 + c_1c_2$ and $a_1c_2 + c_1a_2$ as well. By Lemma 5.2 this is impossible. In conclusion, (5.2) implies that q^{2l} divides either $a_1c_2 - c_1a_2$ or $a_1a_2 - c_1c_2$, as claimed. \square

5.5 Corollary There exists a unique factorization $m = fg$, where f and g are positive, relatively prime integers, such that

$$f^2 \text{ divides } a_1c_2 - c_1a_2 \text{ and } g^2 \text{ divides } a_1a_2 - c_1c_2.$$

Moreover, f is relatively prime to $a_1a_2 - c_1c_2$, while g is relatively prime to $a_1c_2 - c_1a_2$.

Proof This follows immediately from Lemma 5.3 and 5.4. \square

Remark Notice that the factorization in Corollary 5.5 is trivial if $\{a_1, c_1\} = \{a_2, c_2\}$. In this case we have $\{f, g\} = \{1, m\}$.

From now on we shall assume that we have two distinct Markoff triples with a common dominant member. So we suppose that

$$\{a_1, c_1\} \cap \{a_2, c_2\} = \emptyset$$

This implies that $a_1c_1 - a_2c_2 = b_1 - b_2 \neq 0$, and hence $a_1c_2 - c_1a_2 \neq 0$, $a_1a_2 - c_1c_2 \neq 0$, by (5.2).

5.6 Lemma Both, f and g have at least one prime factor which is not equal to 2 or 3, respectively.

Proof Suppose that one of the two factors, g say, does not have a prime factor other than 2 or 3. If m is odd, then m^2 divides $a_1c_2 - c_1a_2$, which is non-zero by our assumption. This implies $m^2 < a_1c_2$ or $m^2 < c_1a_2$. In either case, m is smaller than at least one of the four numbers a_1, c_1, a_2, c_2 , which is impossible. If m is even, then a_1, c_1, a_2, c_2 are odd, and so $a_1c_2 - c_1a_2$ is even. It follows that $\frac{m^2}{2}$ divides $a_1c_2 - c_1a_2$. As in the reasoning above we infer that $\frac{m}{\sqrt{2}}$ is less than at least one of the four numbers a_1, c_1, a_2, c_2 , which is impossible since the dominant member of a Markoff triple exceeds the others by at least a factor $\frac{3}{2}$. Finally, if f does not have a prime factor other than 2 or 3, we apply the same line of reasoning to $a_1a_2 - c_1c_2$, which is also non-zero by our assumption, thus leading to a contradiction as well. \square

We shall now return to the representation (3.4), introducing the following notation. Writing temporarily

$$N(a_1, b_1, c_1, a_2, b_2, c_2, s) = N(s),$$

we define for $i, j \in \{\pm 1, \pm 2\}$,

$$N_{(i,j)}(s) = \begin{cases} N(a_i, b_i, c_i, a_j, b_j, c_j, s) & \text{if } i, j > 0 \\ N(c_i, b_i, a_i, a_j, b_j, c_j, s) & \text{if } i < 0, j > 0 \\ N(a_i, b_i, c_i, c_j, b_j, a_j, s) & \text{if } i > 0, j < 0 \\ N(c_i, b_i, a_i, c_j, b_j, a_j, s) & \text{if } i, j < 0 \end{cases}$$

For $i, j \in \{\pm 1, \pm 2\}$ we define the matrices R_i in a similar fashion.

Remark Recalling that $\mathcal{J} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, one can show that $\mathcal{J}_i = \mathcal{J}N_{(i,-i)}(0)$ is nothing but the involution which is uniquely determined by the identities $\mathcal{J}_i R_i \mathcal{J}_i = -R_i$, $\mathcal{J}_i \mathcal{J} = \mathcal{J} \mathcal{J}_{-i}$.

The next statement specifies the values of the rational numbers s for which the matrix $N_{(1,2)}(s)$ is integral.

5.7 Lemma If $N_{(1,2)}(s^*) \in \mathbf{M}_3(\mathbb{Z})$, then $s^* = \frac{n^*}{3m}$, where n^* solves the diophantine equation

$$(5.3)$$

$$f c_1 n^* + g k^* = -2a_1, \text{ in case } m \text{ is odd, and } f c_1 n^* + g k^* = -a_1 \text{ in case } m \text{ is even}$$

Proof Suppose that m is odd. First we are going to show that any rational number s such that $N_{(1,2)}(s) \in \mathbf{M}_3(\mathbb{Z})$ is of the form $s = \frac{n}{9g}$, where n and g are relatively prime. The assumption $N_{(1,2)}(s) = N(s) \in \mathbf{M}_3(\mathbb{Z})$ implies

$$S_2 N(s) = \frac{1}{m}(\Omega_0 + m\Omega_1) + s\Phi^t \in \mathbf{M}_3(\mathbb{Z}),$$

hence

$$\frac{1}{m}\Omega_0 + s\Phi^t \in \mathbf{M}_3(\mathbb{Z}).$$

Since each entry of Ω_0 is divisible by 9 in case m is odd, and by 18 in case m is even, it follows from Corollary 3.5 and Lemma 3.3 a)

$$\frac{1}{g}\Omega_0 + s\Phi^t \in \mathbf{M}_3(\mathbb{Z})$$

and this implies

$$s\Phi^t \in \frac{1}{g}\mathbf{M}_3(\mathbb{Z}).$$

Since the greatest common divisor of all the entries of the matrix Φ^t is 9, we infer that $s \in \frac{1}{9g}\mathbb{Z}$, as claimed. By Corollary 5.5 the entries of Ω_0 and g are relatively prime. Therefore, n and g have to be relatively prime as well. We shall now give two proofs for the determination of the numerator n^* in the reduced fraction s .

Our first proof relies on the following factorization, which is a consequence of (4.1):

$$N_{(1,-1)}\left(\frac{n}{9g}\right) = N_{(2,-1)}(0)N_{(1,2)}\left(\frac{n}{9g}\right).$$

Since $N_{(1,2)}\left(\frac{n}{9g}\right) \in \text{SL}(3, \mathbb{Z})$ by assumption, while $N_{(2,-1)}(0) \in \frac{1}{f^2}\mathbf{M}_3(\mathbb{Z})$ we know that

$$N_{(1,-1)}\left(\frac{n}{9g}\right) \in \frac{1}{f^2}\mathbf{M}_3(\mathbb{Z}).$$

Adding entry (3,1) and (1,3) in the matrix $N_{(1,-1)}\left(\frac{n}{9g}\right)$ yields

$$a_1^2 \frac{n}{9g} + \frac{1}{2} \left(\frac{n^2}{81g^2} - \frac{n}{9g} \right) (a_1^2 + c_1^2) = a_1^2 \frac{n}{9g} + \frac{1}{2} \left(\frac{n^2}{81g^2} - \frac{n}{9g} \right) b_1 m \epsilon \frac{1}{f^2} \mathbb{Z}$$

In case m is odd, this in turn leads to

$$a_1^2 \frac{n}{g} + \frac{1}{2} b_1 f \frac{n^2}{9g} \epsilon \frac{1}{2f^2} \mathbb{Z}.$$

Since 3 is not a factor of fg , this entails that n is divisible by 3. Let $n^* = \frac{n}{3}$. Then

$$(6a_1^2 + b_1 f n^*) \frac{n^*}{g} \epsilon \frac{1}{f^2} \mathbb{Z}.$$

Since f and g are relatively prime, we infer from this

$$(6a_1^2 + b_1 f n^*) \frac{n^*}{g} \epsilon \mathbb{Z}.$$

Since n and g are relatively prime, we obtain

$$\frac{6a_1^2 + b_1 f n^*}{g} \epsilon \mathbb{Z}.$$

Finally, invoking the identity $b_1 = 3a_1c_1 - fg$ shows that n^* has the claimed property.

Our second proof relies on the observation that the second column in the matrix

$N_{(1,2)}(0)$ is the unit vector $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$. By assumption we must have

$$N_{(1,2)}\left(\frac{n}{9g}\right) \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = e^{-\frac{R_2}{2} \frac{n}{9g}} N_{(1,2)}(0) \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = e^{-\frac{R_2}{2} \frac{n}{9g}} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \epsilon \mathbb{Z}^3.$$

For the first component of this vector we get in case m is an odd Markoff number,

$$(mc_2 - 2a_2)\frac{n}{18g} + mc_2\frac{n^2}{162g^2}\epsilon\mathbb{Z},$$

or

$$\frac{f\mathfrak{c}_2}{2} - \frac{\mathfrak{a}_2n}{3g} + f\mathfrak{c}_2\frac{n^2}{18g}\epsilon\mathbb{Z}.$$

Since neither f nor \mathfrak{c}_2 are divisible by 3, n has to be divisible by 3. Let $n^* = \frac{n}{3}$. Then we get

$$\frac{f\mathfrak{c}_2}{2} - \frac{\mathfrak{a}_2n^*}{g} + f\mathfrak{c}_2\frac{(n^*)^2}{2g}\epsilon\mathbb{Z},$$

hence,

$$(-2\mathfrak{a}_2 + f\mathfrak{c}_2n^*)\frac{n^*}{2g}\epsilon\mathbb{Z}.$$

Since n^* and g are relatively prime, this entails

$$-2\mathfrak{a}_2 + f\mathfrak{c}_2n^*\epsilon g\mathbb{Z}.$$

By Corollary 3.5 this implies

$$-2\mathfrak{c}_1 + f\mathfrak{a}_1n^*\epsilon g\mathbb{Z}.$$

Finally, by virtue of the Markoff property we infer from this,

$$2\mathfrak{a}_1 + f\mathfrak{c}_1n^*\epsilon g\mathbb{Z},$$

thus concluding the argument. If m is even, then the above proofs carry over with some obvious factor 2 adjustments. \square

Remark There is a connection between the second proof of the determination of the numerator n^* and the the case $q = m$ in Proposition 4.6 which is apt to shed some light on the arguments that follow below. By (4.2) the matrix $W(a, b, c)$ is a solution of the system (4.9) and (4.10). Therefore, by Proposition 3.1, any (integral) solution of the system (4.9) and (4.10) must have the form $e^{-\frac{R}{2}s}W$. In order to determine the rational parameter s , exactly the same line of reasoning as in the second proof above leads to the conclusion that s has always the same form as s^* for a suitable factorization of m . While the proofs in these two situations is identical, the respective context is markedly distinct, as is apparent from a comparison of the first proof given above with the second one. Both of these two proofs should be compared with the arguments unfolding below.

We shall now proceed to the proof of the Theorem. For convenience we shall consider odd Markoff numbers m only, the case of an even m requiring occasionally some obvious factor 2 adjustment. Let $\mathfrak{m} = \frac{m}{3}$. First we choose n^* and k^* as in Lemma 5.7. By Lemma 5.1 there exists an integer n_1 such that

(5.4)

$$n_1^2 + 1 = \mathfrak{m}l_1; c_1n_1 - a_1 = gv, v \in \mathbb{Z}; g \text{ and } v \text{ relatively prime.}$$

Next we replace the integer α in the matrix \mathcal{A} occurring in Proposition 4.6 by n_1 , denoting the resulting matrix by \mathcal{A}_1 . The following observation is crucial.

Lemma 5.8 All the reduced fractions in the second column of the matrix

$$\begin{aligned} Z(a_1, b_1, c_1)^{-1} \mathcal{A}_1 &= \frac{1}{2m^2} \begin{pmatrix} -2c_1 & 2a_1 - mc_1 & mc_1 \\ 2a_1c_1 & c_1^2 - a_1^2 & -mb_1 \\ -2a_1 & ma_1 - 2c_1 & ma_1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -n_1 & m & 0 \\ \frac{l_1}{3} & -2n_1 & m \end{pmatrix} = \\ &= \frac{1}{2m^2} \begin{pmatrix} -2(c_1 + a_1n_1) + mc_1(\frac{l_1}{3} + n_1) & 2m(a_1 - c_1n_1) - m^2c_1 & m^2c_1 \\ 2a_1c_1 - n_1(c_1^2 - a_1^2) - mb_1\frac{l_1}{3} & m(c_1^2 - a_1^2 + 2b_1n_1) & -m^2b_1 \\ 2(c_1n_1 - a_1) + ma_1(\frac{l_1}{3} - n_1) & m^2a_1 - 2m(c_1 + a_1n_1) & m^2a_1 \end{pmatrix} \end{aligned}$$

have a denominator which is equal to f or $2f$.

For the first entry in the second column this is obvious, and for the other two it follows by means of the Markoff property. Next we consider the first identity in (4.28) with the choices $\alpha_1 = n_1, \alpha_2 = n_1 + fn^*$, yielding

(5.5)

$$\begin{pmatrix} 1 & 0 & 0 \\ -n_1 & m & 0 \\ \frac{l_1}{3} & -2n_1 & m \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -\frac{n^*}{3g} & 1 & 0 \\ (\frac{n^*}{3g})^2 & -2\frac{n^*}{3g} & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -(n_1 + fn^*) & m & 0 \\ \frac{1}{3}(l_1 + 2n_1\frac{n^*}{g} + \frac{f(n^*)^2}{g}) & -2(n_1 + fn^*) & m \end{pmatrix}.$$

We claim that the term

(5.6)

$$2n_1\frac{n^*}{g} + \frac{f(n^*)^2}{g} = \frac{n^*}{g}(2n_1 + fn^*)$$

in the last entry of the first column of the matrix on the right hand side of (5.5) is an integer. To see this, we multiply the second equation in (5.4) by 2 and add the result to the first identity in (5.3), obtaining,

$$c_1(2n_1 + fn^*) = g(2u - k^*).$$

But since c_1 and g are relatively prime, the integer c_1 has to divide the integer $2u - k^*$, and therefore the rational number in (5.6) is indeed an integer, as claimed. In conclusion, letting

$$n_2 = n_1 + fn^*, l_2 = l_1 + 2n_1\frac{n^*}{g} + \frac{f(n^*)^2}{g},$$

we have found that

$$(n_2)^2 + 1 = \mathbf{m}l_2; n_2, l_2 \in \mathbb{Z}.$$

By Lemma 5.1 here exists a factorization $\mathbf{m} = pq$ into relatively prime factors such that

(5.7)

$$c_2n_2 - a_2 = qv, v \in \mathbb{Z}; p \text{ and } v \text{ relatively prime.}$$

Let

$$\mathcal{A}_2 = \begin{pmatrix} 1 & 0 & 0 \\ -n_2 & m & 0 \\ \frac{l_2}{3} & -2n_2 & m \end{pmatrix}.$$

Since

$$N(0) = Z(a_2, b_2, c_2)^{-1} Z(a_1, b_1, c_1),$$

we obtain

$$N\left(\frac{n^*}{3g}\right) Z(a_1, b_1, c_1)^{-1} \mathcal{A}_1 = e^{-\frac{R_2}{2} \frac{n^*}{3g}} N(0) Z(a_1, b_1, c_1)^{-1} \mathcal{A}_1 = e^{-\frac{R_2}{2} \frac{n^*}{3g}} Z(a_2, b_2, c_2)^{-1} \mathcal{A}_1$$

Since

$$R_2 Z(a_2, b_2, c_2)^{-1} = Z(a_2, b_2, c_2)^{-1} \begin{pmatrix} 0 & 0 & 0 \\ 2m & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix},$$

this is equal to

$$Z(a_2, b_2, c_2)^{-1} \exp\left(\frac{n^*}{6g} \begin{pmatrix} 0 & 0 & 0 \\ 2m & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}\right) \mathcal{A}_1 = Z(a_2, b_2, c_2)^{-1} \exp\left(\frac{n^*}{3g} \begin{pmatrix} 0 & 0 & 0 \\ m & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}\right) \mathcal{A}_1,$$

and since

$$\begin{pmatrix} 0 & 0 & 0 \\ m & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \mathcal{A}_1 = \mathcal{A}_1 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

this in turn is equal to

$$Z(a_2, b_2, c_2)^{-1} \mathcal{A}_1 \exp\left(\frac{n^*}{3g} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}\right) = Z(a_2, b_2, c_2)^{-1} \mathcal{A}_2 =$$

$$\frac{1}{2m^2} \begin{pmatrix} -2(c_2 + a_2n_2) + mc_2(n_2 + \frac{l_2}{3}) & 2m(a_2 - c_2n_2) - m^2c_2 & m^2c_2 \\ 2a_2c_2 - n_2(c_2^2 - a_2^2) - mb_1\frac{l_2}{3} & m(c_2^2 - a_2^2 + 2b_2n_2) & -m^2b_2 \\ 2(c_1n_2 - a_2) + ma_2(\frac{l_2}{3} - n_2) & m^2a_2 - 2m(c_2 + a_2n_2) & m^2a_2 \end{pmatrix}.$$

But since $N(\frac{n^*}{3g}) \in \text{SL}(3, \mathbb{Z})$, by evaluating the second columns only, it follows from Lemma 5.8 that the denominator of each of the reduced fractions in the three entries of the second column of this matrix is a divisor of $2f$, and at least one is equal to f or $2f$. By virtue of the Markoff property it follows

that all three entries of the second column, in particular the first one, have a denominator which is either equal to f or $2f$. This in turn implies that the factor q in (5.7) has to be equal to g , due to the fact that we are considering reduced fraction only. Now

$$c_2 n_2 - a_2 = 0 \text{ modulo } 3g$$

implies, by Corollary 5.5,

$$a_1 n_2 - c_1 = 0 \text{ modulo } 3g,$$

which in turn implies, by the Markoff property,

$$c_1 n_2 + a_1 = 0 \text{ modulo } 3g.$$

Comparing this with (5.4), and invoking once again Lemma 5.1, leads to the conclusion that,

$$n_1 + n_2 = 0 \text{ modulo } \mathfrak{m}.$$

This means that for some integer j we have,

$$\frac{n_1}{\mathfrak{m}} - \frac{n^*}{g} = \frac{n_2}{\mathfrak{m}} = -\frac{n_1}{\mathfrak{m}} + j\mathfrak{m},$$

or

$$\frac{2n_1}{\mathfrak{m}} = \frac{n^*}{g} + j\mathfrak{m}.$$

Since n_1 and \mathfrak{m} are relatively prime, and since g is a proper factor of \mathfrak{m} , this is impossible, and we have reached a contradiction, thus proving the Theorem.

6 Determination of the matrix $Z^{\text{adj}}\mathcal{A}$

In this section we embark on a refined analysis of the matrix

(6.1)

$$\begin{aligned} Z^{\text{adj}}\mathcal{A} &= \begin{pmatrix} -2c & 2a - mc & mc \\ 2ac & c^2 - a^2 & -mb \\ -2a & ma - 2c & ma \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -\alpha & m & 0 \\ \frac{l}{3} & -2\alpha & m \end{pmatrix} = \\ &= \begin{pmatrix} -2(c + a\alpha) + mc(\frac{l}{3} + \alpha) & 2m(a - c\alpha) - m^2c & m^2c \\ 2ac - (c^2 - a^2)\alpha - mb\frac{l}{3} & m(c^2 - a^2 + 2b\alpha) & -m^2b \\ 2(c\alpha - a) + ma(\frac{l}{3} - \alpha) & m^2a - 2m(c + a\alpha) & m^2a \end{pmatrix}, \end{aligned}$$

which appeared in Proposition 4.6. Let $\mathfrak{m} = \frac{m}{3}$. Since $\det(Z^{-1}\mathcal{A}) = \frac{1}{2}$ it follows from (4.24) that all entries in this matrix are divisible by \mathfrak{m}^2 . This is trivially

true for the entries in last column. By the specification of α in Proposition 4.6 and by the Markoff property this is also clear for the entries in the second column. Also by virtue of the Markoff property, the divisibility by \mathfrak{m}^2 of any of the three entries in the first column implies the divisibility by \mathfrak{m}^2 of the other two entries. As we shall see, the divisibility by \mathfrak{m}^2 of any (and hence all) of the three entries in the first column, holds significant number theoretic information. First, however, for the purpose of transparency, we are going to change the notations in Proposition 4.6 for the quadratic residues, to the effect that they reflect the respective Markoff numbers they are affiliated with. Letting $k_m = \alpha$, $k_c = k$, by the Markoff property there exists always an integer k_a such that

$$(6.2) \quad ck_m - mk_c = a, mk_a - ak_m = c.$$

Moreover, again by the Markoff property, there exist positive integers l_a, l_m, l_c such that

$$(6.3) \quad k_a^2 + 1 = \mathfrak{a}l_a, k_m^2 + 1 = \mathfrak{m}l_m, k_c^2 + 1 = \mathfrak{c}l_c.$$

Below we are going to restrict the values of these parameters. With this notation in place we shall prove,

6.1 Proposition The following identities hold true,

$$(6.4) \quad \begin{aligned} k_m l_a - k_a l_m &= l_c + 3k_c, k_c l_m - k_m l_c = l_a - 3k_a, \\ \mathfrak{m}l_a - \mathfrak{a}l_m &= 2k_c + 3\mathfrak{c}, \mathfrak{c}l_m - \mathfrak{m}l_c = 2k_a - 3\mathfrak{a}. \end{aligned}$$

Remarks 1) Rewriting the first and the last entry in the first column of the matrix in (6.1) in terms of the notation introduced in (6.3) and (6.4) one can see that the first identity in (6.4) implies the divisibility by $m\mathfrak{m}$ of the first entry, while the second identity in (6.4) implies the divisibility by $m\mathfrak{m}$ of the third entry. As the proof of Proposition 6.1 will show, however, the identities in (6.4) are equivalent to these two respective divisibility properties.

2) The first two identities in (6.4) appear in [F], *Gesammelte Abhandlungen* Band III, p. 604 (18.) without proof.

The proof of Proposition 6.1 will be based on several lemmas which we are now going to tackle. For any integer x let

$$(6.5) \quad k_a(x) = k_a + \mathfrak{a}x, k_m(x) = k_m + \mathfrak{m}x, k_c(x) = k_c + \mathfrak{c}x;$$

(6.6)

$$l_a(x) = l_a + 2k_ax + \mathfrak{a}x^2, l_m(x) = l_m + 2k_mx + \mathfrak{m}x^2, l_c(x) = l_c + 2k_cx + \mathfrak{c}x^2.$$

Abusing the terminology somewhat, we use in each instant the same symbol for the polynomial as well as its constant term. This should not give rise to any confusion because we will throughout denote the polynomial by the respective symbol followed by (x) . If the constants $\alpha = k_m$ and $l = l_m$ in the matrix $Z^{\text{adj}}\mathcal{A}$ in (6.1) are replaced by the polynomials $k_m(x)$ and $l_m(x)$, respectively, then the resulting polynomial matrix

(6.7)

$$\begin{pmatrix} -2(c + ak_m(x)) + mc(\frac{l_m(x)}{3} + k_m(x)) & 2m(a - ck_m(x)) - m^2c & m^2c \\ 2ac - (c^2 - a^2)k_m(x) - mb\frac{l_m(x)}{3} & m(c^2 - a^2 + 2bk_m(x)) & -m^2b \\ 2(ck_m(x) - a) + ma(\frac{l_m(x)}{3} - k_m(x)) & m^2a - 2m(c + ak_m(x)) & m^2a \end{pmatrix} =$$

$$\begin{pmatrix} [-2k_a(x) + c(k_m + \frac{l_m(x)}{3})]m & 2m(a - ck_m(x)) - m^2c & m^2c \\ 2ac - (c^2 - a^2)k_m(x) - mb\frac{l_m(x)}{3} & m(c^2 - a^2 + 2bk_m(x)) & -m^2b \\ [2k_c(x) + a(\frac{l_m(x)}{3} - k_m(x))]m & m^2a - 2m(c + ak_m(x)) & m^2a \end{pmatrix}$$

has still the property that every entry is divisible by \mathfrak{m}^2 for all $x \in \mathbb{Z}$. Considering the entries (1,1) and (3,1), respectively, it follows that there exists integer valued functions $u_a(x)$ and $u_c(x)$ such that

(6.8)

$$\begin{aligned} \mathfrak{m}^2 u_c(x) &= -2(\mathfrak{c} + ak_m(x)) + \mathfrak{m}c(l_m(x) + 3k_m(x)), \\ \mathfrak{m}^2 u_a(x) &= 2(\mathfrak{c}k_m(x) - \mathfrak{a}) + \mathfrak{m}a(l_m(x) - 3k_m(x)) \end{aligned}$$

or alternatively

(6.9)

$$\mathfrak{m}u_c(x) = -2k_a(x) + \mathfrak{c}(l_m(x) + 3k_m(x)), \mathfrak{m}u_a(x) = 2k_c(x) + \mathfrak{a}(l_m(x) - 3k_m(x))$$

6.2 Lemma The functions $u_a(x)$ and $u_c(x)$ are quadratic polynomials with integral coefficients which have the form

(6.10)

$$u_a(x) = \mathfrak{a}x^2 + (2k_a - 3\mathfrak{a})x + u_a, u_c(x) = \mathfrak{c}x^2 + (2k_c + 3\mathfrak{c})x + u_c,$$

where u_a and u_c are integers.

Proof Obviously, the expressions on the right hand side of the two identities in (6.9) are quadratic polynomials, and therefore the functions $u_a(x)$ and $u_c(x)$

are quadratic polynomials as well, which, by virtue of the divisibility properties of the entries in the matrix (6.7), must have integral coefficients. So, if $u_a(x) = u_a^{(2)}x^2 + u_a^{(1)}x + u_a$, then (6.5), (6.6) and the second identity in (6.9) yield

$$\mathfrak{m}(u_a^{(2)}x^2 + u_a^{(1)}x + u_a) = \mathfrak{m}ax^2 + (2\mathfrak{c} + 2\mathfrak{a}k_m - 3\mathfrak{a}m)x + 2k_c + \mathfrak{a}l_m - 3\mathfrak{a}k_m,$$

which in turn, by the second identity in (6.2), is equal to

$$\mathfrak{m}ax^2 + \mathfrak{m}(2k_a - 3\mathfrak{a})x + 2k_c + \mathfrak{a}l_m - 3\mathfrak{a}k_m.$$

Comparing the coefficients on both sides, we get,

$$u_a^{(2)} = \mathfrak{a}, u_a^{(1)} = 2k_a - 3\mathfrak{a},$$

as claimed. The second identity in (6.10) can be settled in a similar way. \square

Let

$$(6.11) \quad v_a(x) = u_a(x) + 3k_a(x), v_c(x) = u_c(x) - 3k_c(x)$$

6.3 Lemma The following identity holds true,

$$(6.12) \quad \begin{pmatrix} k_m(x) & 1 \\ -1 & k_m(x) \end{pmatrix} \begin{pmatrix} v_a(x) \\ -v_c(x) \end{pmatrix} = \begin{pmatrix} 3 & l_m(x) \\ -l_m(x) & -3 \end{pmatrix} \begin{pmatrix} k_c(x) \\ k_a(x) \end{pmatrix}$$

Proof First, the identities in (6.8) can be written as a linear system in \mathfrak{a} and \mathfrak{c} ,

$$\begin{pmatrix} -\mathfrak{m}(l_m(x) - 3k_m(x)) + 2 & -2k_m(x) \\ -2k_m(x) & \mathfrak{m}(l_m(x) + 3k_m(x)) - 2 \end{pmatrix} \begin{pmatrix} \mathfrak{a} \\ \mathfrak{c} \end{pmatrix} = \mathfrak{m}^2 \begin{pmatrix} -u_a(x) \\ u_c(x) \end{pmatrix}.$$

The determinant of the matrix on the left hand side is equal to

$$\mathfrak{m}^2(9k_m(x)^2 - l_m(x)^2).$$

Hence solving the above linear sytem for $\begin{pmatrix} \mathfrak{a} \\ \mathfrak{c} \end{pmatrix}$ yields,

$$(6.13) \quad \left[2 \begin{pmatrix} -1 & k_m(x) \\ k_m(x) & 1 \end{pmatrix} + \mathfrak{m} \begin{pmatrix} l_m(x) + 3k_m(x) & 0 \\ 0 & -l_m(x) + 3k_m(x) \end{pmatrix} \right] \begin{pmatrix} -u_a(x) \\ u_c(x) \end{pmatrix} = (9k_m(x)^2 - l_m(x)^2) \begin{pmatrix} \mathfrak{a} \\ \mathfrak{c} \end{pmatrix}.$$

By (6.2),

$$\begin{pmatrix} -1 & k_m(x) \\ k_m(x) & 1 \end{pmatrix} \begin{pmatrix} \mathfrak{a} \\ \mathfrak{c} \end{pmatrix} = \mathfrak{m} \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix},$$

or equivalently,

$$\begin{pmatrix} \mathfrak{a} \\ \mathfrak{c} \end{pmatrix} = \frac{1}{l_m(x)} \begin{pmatrix} -1 & k_m(x) \\ k_m(x) & 1 \end{pmatrix} \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix}.$$

Substituting this into (6.13) and multiplying the result from the left by the inverse of the matrix on the right hand side yields,

$$\begin{aligned} & \left[2l_m(x) \begin{pmatrix} 10 \\ 01 \end{pmatrix} + \begin{pmatrix} -l_m(x) - 3k_m(x) & -k_m(x)l_m(x) + 3k_m^2(x) \\ k_m(x)l_m(x) + 3k_m^2(x) & -l_m(x) + 3k_m(x) \end{pmatrix} \right] \begin{pmatrix} -u_a(x) \\ u_c(x) \end{pmatrix} = \\ & (9k_m(x)^2 - l_m(x)^2) \begin{pmatrix} -k_{\mathfrak{c}}(x) \\ -k_{\mathfrak{a}}(x) \end{pmatrix}, \end{aligned}$$

or

$$\begin{pmatrix} l_m(x) - 3k_m(x) & -k_m(x)l_m(x) + 3k_m^2(x) \\ k_m(x)l_m(x) + 3k_m^2(x) & l_m(x) + 3k_m(x) \end{pmatrix} \begin{pmatrix} u_a(x) \\ -u_c(x) \end{pmatrix} = (9k_m(x)^2 - l_m(x)^2) \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix},$$

which, since the matrix on the left hand side is equal to the product

$$\begin{pmatrix} l_m(x) - 3k_m(x) & 0 \\ 0 & l_m(x) + 3k_m(x) \end{pmatrix} \begin{pmatrix} 1 & -k_m(x) \\ k_m(x) & 1 \end{pmatrix},$$

is equivalent to

$$\begin{pmatrix} 1 & -k_m(x) \\ k_m(x) & 1 \end{pmatrix} \begin{pmatrix} u_a(x) \\ -u_c(x) \end{pmatrix} = \begin{pmatrix} l_m(x) + 3k_m(x) & 0 \\ 0 & l_m(x) - 3k_m(x) \end{pmatrix} \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix}.$$

This in turn leads to

$$\begin{aligned} & (k_m^2(x) + 1) \begin{pmatrix} u_a(x) \\ -u_c(x) \end{pmatrix} = \\ & \begin{pmatrix} 1 & k_m(x) \\ -k_m(x) & 1 \end{pmatrix} \begin{pmatrix} l_m(x) + 3k_m(x) & 0 \\ 0 & l_m(x) - 3k_m(x) \end{pmatrix} \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix} = \\ & \begin{pmatrix} l_m(x) + 3k_m(x) & k_m(x)l_m(x) - 3k_m^2(x) \\ -k_m(x)l_m(x) - 3k_m^2(x) & l_m(x) - 3k_m(x) \end{pmatrix} \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix} = \\ & \begin{pmatrix} l_m(x) + 3k_m(x)k_m(x)l_m(x) + 3 - 3(k_m^2(x) + 1) & \\ -k_m(x)l_m(x) + 3 - 3(k_m^2(x) + 1) & l_m(x) - 3k_m(x) \end{pmatrix} \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix} = \\ & \left[\begin{pmatrix} l_m(x) + 3k_m(x)k_m(x)l_m(x) + 3 & \\ -k_m(x)l_m(x) + 3 & l_m(x) - 3k_m(x) \end{pmatrix} - 3(k_m^2(x) + 1) \begin{pmatrix} 01 \\ 10 \end{pmatrix} \right] \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix}. \end{aligned}$$

This entails,

$$(k_m^2(x) + 1) \left[\begin{pmatrix} u_a(x) \\ -u_c(x) \end{pmatrix} + 3 \begin{pmatrix} k_{\mathfrak{a}}(x) \\ k_{\mathfrak{c}}(x) \end{pmatrix} \right] = \begin{pmatrix} k_m(x) & -1 \\ 1 & k_m(x) \end{pmatrix} \begin{pmatrix} 3 & l_m(x) \\ -l_m(x) & -3 \end{pmatrix} \begin{pmatrix} k_{\mathfrak{c}}(x) \\ k_{\mathfrak{a}}(x) \end{pmatrix},$$

and finally, after multiplying this from the left by the inverse of the matrix $\begin{pmatrix} k_m(x) & -1 \\ 1 & k_m(x) \end{pmatrix}$,

$$\begin{pmatrix} k_m(x) & 1 \\ -1 & k_m(x) \end{pmatrix} \left[\begin{pmatrix} u_a(x) \\ -u_c(x) \end{pmatrix} + 3 \begin{pmatrix} k_a(x) \\ k_c(x) \end{pmatrix} \right] = \begin{pmatrix} 3 & l_m(x) \\ -l_m(x) & -3 \end{pmatrix} \begin{pmatrix} k_c(x) \\ k_a(x) \end{pmatrix},$$

which is the claimed identity (3.12) \square

6.4 Lemma The following identity holds true

(6.14)

$$\begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix} \begin{pmatrix} \mathfrak{c} \\ -\mathfrak{b} \\ \mathfrak{a} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

Proof Squaring the two entries of the vector on the left hand side of (6.12), and adding the results together yields,

$$\begin{aligned} (k_m(x)v_a(x) - v_c(x))^2 + (v_a(x) + k_m(x)v_c(x))^2 &= (k_m(x)^2 + 1)(v_a(x)^2 + v_c(x)^2) \\ &= \mathfrak{m}l_m(x)(v_a(x)^2 + v_c(x)^2). \end{aligned}$$

Doing the same thing for the vector on the right hand side yields,

$$\begin{aligned} (k_a(x)l_m(x) - 3k_c(x))^2 + (k_c(x)l_m(x) - 3k_a(x))^2 \\ 9(k_a(x)^2 + k_c(x)^2) + (k_a^2(x)l_m(x) + k_c^2(x)l_m(x) - 12k_a(x)k_c(x))l_m(x). \end{aligned}$$

Therefore, by (6.12),

(6.15)

$$\mathfrak{m}l_m(x)(v_a(x)^2 + v_c(x)^2) = 9(k_a(x)^2 + k_c(x)^2) + (k_a^2(x)l_m(x) + k_c^2(x)l_m(x) - 12k_a(x)k_c(x))l_m(x).$$

It follows from this identity that $9(k_a(x)^2 + k_c(x)^2)$ is divisible by $l_m(x)$. But since $l_m(x)$ is always an integer which has only prime factors of the form $4n+1$, for all integers x the integer

$$k_a(x)^2 + k_c(x)^2 = \mathfrak{a}l_a(x) + \mathfrak{c}l_c(x) - 2$$

is divisible by the integer $l_m(x)$. It follows that for all integers x there exists an integer n_x such that

(6.16)

$$\mathfrak{a}(l_a + 2k_ax + \mathfrak{a}x^2) + n_x(l_m + 2k_mx + \mathfrak{m}x^2) + \mathfrak{c}(l_c + 2k_cx + \mathfrak{c}x^2) = 2.$$

This means that the integer valued function n_x is a fraction of two quadratic polynomials, and therefore has to be a constant. To see this, one has to write

this fraction as a constant C plus a rational function $R = \frac{P}{Q}$ with P linear and Q quadratic. Suppose that R is not zero. Substituting a strictly increasing sequence of integers into $C + R$ leads to a sequence of rational numbers which converges to C . This implies that there are rational numbers in the range of n_x which are not integers, thus leading to a contradiction. Comparing the coefficients in (6.16) for the quadratic terms only leads us to the conclusion that $n_x = -\mathfrak{b}$, by virtue of the Markoff property. Comparing the other coefficients as well, leads us finally to the vector identity (6.14) \square

Remark Since $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are relatively prime, it follows from the identity (6.14) that

$$\det \begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix} = \pm 2. \quad \text{This conclusion has already been reached by Frobenius in [F], Gesam-$$

melte Abhandlungen, Band III, p.604 (13.). Even though he does not provide a detailed proof, he refers to the last identity in (9.) on p.603, which is equivalent to (6.16) taking $x = 0, n_x = -\mathfrak{b}$.

6.5 Lemma The following identity holds true

$$(6.17) \quad \mathfrak{a}v_a + \mathfrak{c}v_c = \mathfrak{a}l_a + \mathfrak{c}l_c$$

Proof The proof of Lemma 6.4 shows that (6.15) simplifies to

$$\mathfrak{m}(v_a(x)^2 + v_c(x)^2) = (9 + l_m(x)^2)b + 12k_a k_c.$$

Evaluating this identity for the quadratic terms leads to

$$\mathfrak{m}(2\mathfrak{a}v_a + 4k_a^2 + 2\mathfrak{c}v_c + 4k_c^2) = (2\mathfrak{m}l_m + 4k_m^2)\mathfrak{b} + 12\mathfrak{a}\mathfrak{c},$$

which simplifies to

$$\mathfrak{a}v_a + 2\mathfrak{a}l_a + \mathfrak{c}v_c + 2\mathfrak{c}l_c = 6 + 3\mathfrak{b}l_m.$$

But (6.14) implies

$$\mathfrak{a}l_a + \mathfrak{c}l_c = 2 + \mathfrak{b}l_m,$$

and so the claimed identity follows. \square

The following statement will allow us to make specific choices for the matrix in (6.14). It has been known for a long time and can be found for instance in [R], p.163 (47).

6.6 Lemma The numbers k_a, k_m, k_c in (6.2) can be chosen so that they all have the same sign, and

$$(6.18) \quad |k_a| \leq \frac{\mathfrak{a}}{2}, \quad |k_m| \leq \frac{\mathfrak{m}}{2}, \quad |k_c| \leq \frac{\mathfrak{c}}{2}.$$

The inequalities in (6.18) obviously imply the following,

$$(6.19) \quad l_a \leq \frac{\mathfrak{a}}{4} + \frac{1}{\mathfrak{m}}, \quad l_m \leq \frac{\mathfrak{m}}{4} + \frac{1}{\mathfrak{m}}, \quad l_c \leq \frac{\mathfrak{c}}{4} + \frac{1}{\mathfrak{c}}.$$

Henceforth we shall restrict the parameters in question to those satisfying (6.18).

6.7 Lemma the following identities hold true

$$(6.20) \quad v_a = l_a, \quad v_c = l_c$$

Proof Since, by (6.17),

$$\mathfrak{a}(v_a - l_a) = \mathfrak{c}(l_c - v_c),$$

and since \mathfrak{a} and \mathfrak{c} are relatively prime, we conclude that

$$(6.21) \quad \frac{v_a - l_a}{\mathfrak{c}} \in \mathbb{Z}, \quad \frac{v_c - l_c}{\mathfrak{a}} \in \mathbb{Z}.$$

By (6.12),

$$\begin{aligned} \begin{pmatrix} v_a(x) \\ -v_c(x) \end{pmatrix} &= \frac{1}{\mathfrak{m}l_m} \begin{pmatrix} k_m - 1 \\ 1 & k_m \end{pmatrix} \begin{pmatrix} 3 & l_m \\ -l_m & -3 \end{pmatrix} \begin{pmatrix} -k_c \\ k_a \end{pmatrix} \\ &= \frac{1}{\mathfrak{m}l_m} \begin{pmatrix} l_m + 3k_mk_ml_m + 3 \\ -k_ml_m + 3 & l_m - 3k_m \end{pmatrix} \begin{pmatrix} -k_c \\ k_a \end{pmatrix}, \end{aligned}$$

in particular

$$(6.22) \quad v_a = \frac{1}{\mathfrak{m}l_m} (-(l_m + 3k_m)k_c + (k_ml_m + 3)k_a)$$

Suppose that $\mathfrak{a} \leq \mathfrak{c} \leq \mathfrak{m}$. We are now going to use (6.18), (6.19) and (6.22) to obtain an upper bound for $|\frac{v_a - l_a}{\mathfrak{c}}|$. First,

$$\left| \frac{l_m + 3k_m}{\mathfrak{m}l_m} \right| \leq \frac{1}{\mathfrak{m}} + 3 \frac{1}{\sqrt{\mathfrak{m}l_m}},$$

$$\left| \frac{k_m l_m + 3}{\mathfrak{m} l_m} \right| \leq \frac{1}{2} + \frac{3}{\mathfrak{m} l_m},$$

and therefore, by (6.22) and (6.18)

$$|v_a| \leq \left(\frac{1}{\mathfrak{m}} + 3 \frac{1}{\sqrt{\mathfrak{m} l_m}} \right) \frac{\mathfrak{c}}{2} + \left(\frac{1}{2} + \frac{3}{\mathfrak{m}} \right) \frac{\mathfrak{a}}{2} \leq \frac{1}{2} \left(\frac{1}{\mathfrak{m}} + 3 \frac{1}{\sqrt{\mathfrak{m} l_m}} + \frac{1}{2} + \frac{3}{\mathfrak{m} l_m} \right) \mathfrak{c}.$$

Hence, by (6.19),

$$\left| \frac{v_a - l_a}{\mathfrak{c}} \right| \leq \frac{|v_a|}{\mathfrak{c}} + \frac{l_a}{\mathfrak{c}} \leq \frac{1}{2} \left(\frac{1}{\mathfrak{m}} + 3 \frac{1}{\sqrt{\mathfrak{m} l_m}} + \frac{1}{2} + \frac{3}{\mathfrak{m} l_m} \right) + \frac{1}{4} + \frac{1}{\mathfrak{a} \mathfrak{c}}.$$

If $\mathfrak{m} \geq 29$, then $\mathfrak{a} \mathfrak{c} \geq 10$, and in this case the right hand side of this inequality is a number which is less than 1. For those Markoff triples which meet this condition, it follows from (6.21) that v_a is equal to l_a , and hence by (6.17), v_c is equal to l_c , settling the claim of the lemma in case $\mathfrak{a} \leq \mathfrak{c} \leq \mathfrak{m}$. If $\mathfrak{c} \leq \mathfrak{a} \leq \mathfrak{m}$, then the same type of estimates for $\left| \frac{v_c - l_c}{\mathfrak{a}} \right|$ in place of $\left| \frac{v_a - l_a}{\mathfrak{c}} \right|$ lead to the same conclusion. For the Markoff triples for which the largest member is less than 29, namely the triples (1,1,1); (1,1,2); (1,2,5) and (1,5,13), the validity of the claim can be checked through inspection. \square

Proof of Proposition 6.1 The first two identities follow from Lemma 6.3 and Lemma 6.7. In order to establish the third identity we reintroduce the parameter x into the first identity, write out the result in terms of x ,

$$(k_m + \mathfrak{m}x)(l_a + 2k_a x + \mathfrak{a}x^2) - (k_a + \mathfrak{a}x)(l_m + 2k_m x + \mathfrak{m}x^2) = l_c + 2k_c + \mathfrak{c}x^2 + 3k_c + 3\mathfrak{c},$$

and compare the coefficients of the linear terms. This yields the third identity. The fourth identity can shown in exactly the same way by employing the second identity. \square

Putting together what has been established so far, we can summarize the situation through the following (incomplete) matrix identities,

(6.23)

$$\begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix}^{-1} = \frac{1}{2} \begin{pmatrix} l_c + 3k_c & -(2k_c + 3\mathfrak{c}) & \mathfrak{c} \\ ? & ? & -\mathfrak{b} \\ l_a - 3k_a & -(2k_a - 3\mathfrak{a}) & \mathfrak{a} \end{pmatrix},$$

(6.24)

$$Z^{-1} \mathcal{A} = \frac{1}{2} \begin{pmatrix} l_c + 3k_c & -(2k_c + 3\mathfrak{c}) & \mathfrak{c} \\ ? & ? & -\mathfrak{b} \\ l_a - 3k_a & -(2k_a - 3\mathfrak{a}) & \mathfrak{a} \end{pmatrix} \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

The factor $\frac{1}{2}$ on the right hand side of (6.23) is a consequence of (6.14). What follows are comments on the seven enunciated entries of the matrix on the right hand side of (6.23). If we consider the x -parameter version of the first identity in (6.4), namely $k_m(x)l_a(x) - k_a(x)l_m(x) = l_c(x) + 3k_c(x)$, then comparing the coefficients of the constant terms yields the entry (1,1), comparing the coefficients of the linear terms yields the entry (1,2), and comparing the coefficients of the quadratic terms yields the entry (1,3) of the matrix on the right hand side in (6.23). Likewise, if we consider the x -parameter version of the second identity in (6.4), namely $k_c(x)l_m(x) - k_m(x)l_c(x) = l_a(x) - 3k_a(x)$, then comparing the coefficients of the constant terms yields the entry (3,1), comparing the coefficients of the linear terms yields the entry (3,2), and comparing the coefficients of the quadratic terms yields the entry (3,3) of the matrix on the right hand side in (6.23). The entry (2,3) is a consequence of (6.14). Turning to the matrix identity (6.24), it suffices to note that this is a consequence of (6.23) and Lemma 6.7.

Our next objective is to obtain more information about the entries (2,1) and (2,2) of the matrix on the right hand side in (6.23). Let

(6.25)

$$\mathcal{A}(c, m, a) = \begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix},$$

$$\mathcal{B}(c, m, a) = \frac{1}{2m^2} \begin{pmatrix} -2(c + ak_m) + mc(\frac{l_m}{3} + k_m) & 2m(a - ck_m) - m^2c & m^2c \\ 2ac - (c^2 - a^2)k_m - mb\frac{l_m}{3} & m(c^2 - a^2 + 2bk_m) & -m^2b \\ 2(ck_m - a) + ma(\frac{l_m}{3} - k_m) & m^2a - 2m(c + ak_m) & m^2a \end{pmatrix}.$$

Note that, due to the specification of the paramters in (6.18), and since $b = ac - m$, both of these matrices are uniquely determined by the Markoff triple (a, m, c) up to the sign chosen in (6.18). Now, instead of (a, m, c) we consider the Markoff triple (a, b, c) in this context. Since $m \geq \max(a, c)$ and $m = ac - b$, we must have $b \leq \max(a, c)$. This means that $\max(a, b, c) \in \{a, c\}$. Suppose $\max(a, b, c) = c$. Then, considering the matrices \mathcal{A} and \mathcal{B} in this context, we have two distinct choices to arrange the members of the triple (a, b, c) , so that the resulting situation is consistent with our settings for (a, m, c) , namely

$$(a, c, b) \text{ or } (b, c, a).$$

In the first case (6.23) and (6.24) turn into, respectively,

$$\mathcal{A}(a, c, b)^{-1} = \frac{1}{2} \begin{pmatrix} l_a + 3k_a & -(2k_a + 3\mathfrak{a}) & \mathfrak{a} \\ ? & ? & -(3\mathfrak{a}\mathfrak{b} - \mathfrak{c}) \\ l_b - 3k_b & -(2k_b - 3\mathfrak{b}) & \mathfrak{b} \end{pmatrix},$$

$$\mathcal{B}(a, c, b) = \frac{1}{2} \begin{pmatrix} l_a + 3k_a & -(2k_a + 3\mathfrak{a}) & \mathfrak{a} \\ ? & ? & -(3\mathfrak{a}\mathfrak{b} - \mathfrak{c}) \\ l_b - 3k_b & -(2k_b - 3\mathfrak{b}) & \mathfrak{b} \end{pmatrix} \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

while we get in the second case,

$$\mathcal{A}(b, c, a)^{-1} = \frac{1}{2} \begin{pmatrix} l_b + 3k_b & -(2k_b + 3\mathfrak{b}) & \mathfrak{b} \\ ? & ? & -(3\mathfrak{a}\mathfrak{b} - \mathfrak{c}) \\ l_a - 3k_a & -(2k_a - 3\mathfrak{a}) & \mathfrak{a} \end{pmatrix}$$

$$\mathcal{B}(b, c, a) = \frac{1}{2} \begin{pmatrix} l_b + 3k_b & -(2k_b + 3\mathfrak{b}) & \mathfrak{b} \\ ? & ? & -(3\mathfrak{a}\mathfrak{b} - \mathfrak{c}) \\ l_a - 3k_a & -(2k_a - 3\mathfrak{a}) & \mathfrak{a} \end{pmatrix} \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Either case leads to the following further specification of (6.23),

(6.26)

$$\begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix}^{-1} = \frac{1}{2} \begin{pmatrix} l_c + 3k_c & -(2k_c + 3\mathfrak{c}) & \mathfrak{c} \\ -(l_b + 3\nu k_b) & 2k_b + 3\nu\mathfrak{b} & -\mathfrak{b} \\ l_a - 3k_a & -(2k_a - 3\mathfrak{a}) & \mathfrak{a} \end{pmatrix}; \nu \in \{-1, 1\}$$

Before proceeding to give a more specific determination of the matrix $Z^{-1}\mathcal{A}$ which involves a certain quadratic equation, we need to look at that equation first.

6.7 Lemma The quadratic equation

(6.27)

$$\mathfrak{m}y^2 - 4\mathfrak{b}k_my - (9\mathfrak{b}^2 - 4)\mathfrak{m} + 4\mathfrak{b}^2l_m - 8\mathfrak{b}\sigma = 0,$$

has always two rational solutions in case $\sigma = 1$, and it has no rational solutions in case $\sigma = -1$.

Proof First we show that the discriminant D of this equation is a perfect square in case $\sigma = 1$.

$$D = 16\mathfrak{b}^2k_m^2 + 4\mathfrak{m}^2(9\mathfrak{b}^2 - 4) - 16\mathfrak{b}^2\mathfrak{m}l_m - 8\mathfrak{b}\mathfrak{m} = -16\mathfrak{b}^2 + 4\mathfrak{m}^2(9\mathfrak{b}^2 - 4) - 8\mathfrak{b}\mathfrak{m}$$

$$\frac{D}{4} = 9\mathfrak{m}^2\mathfrak{b}^2 - 4(\mathfrak{m}^2 + \mathfrak{b}^2) - 8\mathfrak{b}\mathfrak{m} = 9(\mathfrak{a}^2 + \mathfrak{c}^2)^2 - 4(3\mathfrak{a}\mathfrak{c} - \mathfrak{b})^2 - 4\mathfrak{b}^2 - 8(\mathfrak{a}^2 + \mathfrak{c}^2)$$

$$\begin{aligned} &= 9(\mathfrak{a}^4 + 2\mathfrak{a}^2\mathfrak{c}^2 + \mathfrak{c}^4) - 4(9\mathfrak{a}^2\mathfrak{c}^2 - 6\mathfrak{a}\mathfrak{b}\mathfrak{c} + \mathfrak{b}^2) - 4\mathfrak{b}^2 - 8(\mathfrak{a}^2 + \mathfrak{c}^2) \\ &= 9\mathfrak{a}^4 + 18\mathfrak{a}^2\mathfrak{c}^2 + 9\mathfrak{c}^4 - 36\mathfrak{a}^2\mathfrak{c}^2 + 8(\mathfrak{a}^2 + \mathfrak{b}^2 + \mathfrak{c}^2) - 8\mathfrak{b}^2 - 8(\mathfrak{a}^2 + \mathfrak{c}^2) \\ &= 9\mathfrak{a}^4 - 18\mathfrak{a}^2\mathfrak{c}^2 + 9\mathfrak{c}^4 = 9(\mathfrak{a}^2 - \mathfrak{c}^2)^2. \end{aligned}$$

It follows that (6.27) has two rational solutions in case $\sigma = 1$. In order to show that (6.27) does not have a rational solution in case $\sigma = -1$, we are going to show that its discriminant $D + 64\mathfrak{m}\mathfrak{b}$ is not a perfect square, or rather that

$$\frac{D}{4} + 16\mathfrak{m}\mathfrak{b} = 9(\mathfrak{a} + \mathfrak{c})^2(\mathfrak{a} - \mathfrak{c})^2 + 16\mathfrak{m}\mathfrak{b} = 9(\mathfrak{m}\mathfrak{b} + 2\mathfrak{a}\mathfrak{c})(\mathfrak{m}\mathfrak{b} - 2\mathfrak{a}\mathfrak{c}) + 16\mathfrak{m}\mathfrak{b}$$

$$9(\mathfrak{m}^2\mathfrak{b}^2-4\mathfrak{a}^2\mathfrak{c}^2)+16\mathfrak{m}\mathfrak{b}=9\mathfrak{m}^2\mathfrak{b}^2-4(\mathfrak{m}+\mathfrak{b})^2+16\mathfrak{m}\mathfrak{b}=9\mathfrak{m}^2\mathfrak{b}^2-4\mathfrak{m}^2-8\mathfrak{m}\mathfrak{b}-4\mathfrak{b}^2+16\mathfrak{m}\mathfrak{b}$$

$$9\mathfrak{m}^2\mathfrak{b}^2-4(\mathfrak{m}-\mathfrak{b})^2$$

is not a perfect square. Suppose this were false, which means that there exists an integer w such that,

$$4(\mathfrak{m}-\mathfrak{b})^2+w^2=9\mathfrak{m}^2\mathfrak{b}^2.$$

By the standard parametrization of Pythagorean triples there exist then integers u and v such that,

$$\mathfrak{m}-\mathfrak{b}=uv, 3\mathfrak{m}\mathfrak{b}=u^2+v^2.$$

This implies that u^2+v^2 is divisible by 3. However, since u^2+v^2 divided be the square of the greatest common divisor of u and v cannot be divisible by 3, due to the fact that such a number can only have odd prime factors which are equal to 1 modulo 4, both u and v have to be divisible by 3. this in turn implies that $\mathfrak{m}\mathfrak{b}$ has to be divisible by 3, which means that \mathfrak{m} or \mathfrak{b} is divisible by 3. This not the case, because \mathfrak{m} and \mathfrak{b} are Markoff numbers. That contradiction settles our claim. \square

6.8 Proposition The following identity holds true,

(6.28)

$$Z^{-1}\mathcal{A}=\frac{1}{2}\begin{pmatrix} l_c+3k_c & -(2k_c+3\mathfrak{c}) & \mathfrak{c} \\ -(l_b+3\mu k_b) & 2k_b+3\mu\mathfrak{b} & -\mathfrak{b} \\ l_a-3k_a & -(2k_a-3\mathfrak{a}) & \mathfrak{a} \end{pmatrix}\begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

where

(6.29)

$$\mu=\begin{cases} 1 & \text{if } \mathfrak{a} < \mathfrak{c} \\ -1 & \text{if } \mathfrak{a} > \mathfrak{c} \end{cases}$$

Moreover,

(6.30)

$$\det\begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix}=2$$

Proof Note that in each row of the matix $\begin{pmatrix} l_c+3k_c & -(2k_c+3\mathfrak{c}) & \mathfrak{c} \\ -(l_b+3\mu k_b) & 2k_b+3\mu\mathfrak{b} & -\mathfrak{b} \\ l_a-3k_a & -(2k_a-3\mathfrak{a}) & \mathfrak{a} \end{pmatrix}$

the entries represent the coefficients of a binary quadratic form which is equivalent to a Markoff form. For convenience we shall henceforth address the discriminant of a quadratic form whose coefficients agree with the entries of a row

vector as the discriminant of that row. Note that inverting the entries in such a row vector leads to the same discriminant. For instance the second row in the matrix $\begin{pmatrix} l_c + 3k_c & -(2k_c + 3c) & c \\ -(l_b + 3\mu k_b) & 2k_b + 3\mu b & -b \\ l_a - 3k_a & -(2k_a - 3a) & a \end{pmatrix}$ has the discriminant $9b^2 - 4$. We are now going to show that the discriminant of the second row vector in the matrix

$$Z^{-1}\mathcal{A} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{3} \end{pmatrix}$$

has the discriminant $9b^2 - 4$, or equivalently, that the row vector

(6.31)

$$\frac{1}{m}(2ac - (c^2 - a^2)k_m - mb\frac{l_m}{3}, m(3(c^2 - a^2) + 2bk_m), -3m^2b)$$

has the discriminant $m^2(9b^2 - 4)$,

$$\begin{aligned} & \frac{1}{m^2}[(m(3(c^2 - a^2) + 2bk_m))^2 - 4(2ac - (c^2 - a^2)k_m - mb\frac{l_m}{3})(-3m^2b)] = \\ & 3(c^2 - a^2) + 2bk_m)^2 + 4b(6ac - 3(c^2 - a^2)k_m - mbl_m) = \\ & 9(c^2 - a^2)^2 + 12(c^2 - a^2)bk_m + 4b^2k_m^2 + 24abc - 12b(c^2 - a^2)k_m - 4b^2ml_m = \\ & 9(c^2 - a^2)^2 - 4b^2 + 24abc = 9(c + a)^2(c - a)^2 - 4b^2 + 24abc = \\ & 9(mb + 2ac)(mb - 2ac) - 4b^2 + 24abc = 9(m^2b^2 - 4a^2c^2) - 4b^2 + 24abc = \\ & 9m^2b^2 - 12ac(3ac - b) - 4b^2 + 12abc = 9m^2b^2 - 12acm - 4b^2 + 4(a^2 + b^2 + c^2) = \\ & 9m^2b^2 - 12acm + 4bm = 9m^2b^2 - 4m(3ac - b) = m^2(9b^2 - 4). \end{aligned}$$

Let x be the (2,1) entry, and let y be the (2,2) entry in the matrix $\begin{pmatrix} l_c + 3k_c & -(2k_c + 3c) & c \\ ? & ? & -b \\ l_a - 3k_a & -(2k_a - 3a) & a \end{pmatrix}$

in (6.24). Since $\det(\mathcal{A}^{-1}Z) = 2$, it follows from (6.23) and (6.24), as well as the determination of the discriminant of the vector in (6.31), that x and y solve the following two diophantine equations,

$$mx + k_my - bl_m = 2, y^2 + 4bx = 9b^2 - 4.$$

This in turn leads to the quadratic equation (6.27) for the case $\sigma = 1$. The same line of

reasoning applied to the matrix $\begin{pmatrix} l_c + 3k_c & -(2k_c + 3c) & c \\ -(l_b + 3\mu k_b) & 2k_b + 3\mu b & -b \\ l_a - 3k_a & -(2k_a - 3a) & a \end{pmatrix}$ in (6.26)

leads us to a similar conclusion, namely that the second entry in the second row of this matrix solves the quadratic equation (6.27) for $\sigma = 1$ or $\sigma = -1$. But since Lemma 6.7 states that there are no rational solutions to (6.27) in case

$\sigma = -1$, it follows once again that $\sigma = 1$, which settles (6.30). Comparison of the outcome of these two lines of reasoning leads to the conclusion that (6.28) holds true for some $\mu \in \{-1, 1\}$. In order to establish (6.29) we observe that (6.28) evaluated for the entry (2,2) of that matrix yields the following identity,

$$3(\mathfrak{c}^2 - \mathfrak{a}^2) + 2\mathfrak{b}k_m = \mathfrak{m}(2k_{\mathfrak{b}} + 3\mu\mathfrak{b}) = 2\mathfrak{m}k_{\mathfrak{b}} + 3\mu(\mathfrak{c}^2 + \mathfrak{a}^2).$$

This in turn leads to,

$$\mathfrak{b}k_m - \mathfrak{m}k_{\mathfrak{b}} = \begin{cases} 3\mathfrak{a}^2 & \text{if } \mu = 1 \\ -3\mathfrak{c}^2 & \text{if } \mu = -1 \end{cases}.$$

But since

$$|\mathfrak{b}k_m - \mathfrak{m}k_{\mathfrak{b}}| \leq \mathfrak{b}|k_m| + \mathfrak{m}|k_{\mathfrak{b}}| \leq \frac{\mathfrak{m}\mathfrak{b}}{2} + \frac{\mathfrak{m}\mathfrak{b}}{2} = \mathfrak{m}\mathfrak{b} = \mathfrak{c}^2 + \mathfrak{a}^2 \leq 2(\max(\mathfrak{a}, \mathfrak{c}))^2 < 3(\max(\mathfrak{a}, \mathfrak{c}))^2,$$

(6.29) follows. \square

Returning to the settings in the third remark following Proposition 1.2 in section 1 we can now give a conclusive description of the parameter ν in (6.26) in relation to the tree of Markoff triples. First in (6.18) all the parameters are positive (cf. [Z], Lemma 2). If (A, AB, B) is an admissible triple of 2x2 matrices, then the matrix N constructed in Proposition 1.2 such that

$$N^t M(3, 3, 3) N = M(\text{tr}(A), \text{tr}(AB), \text{tr}(B)),$$

has the property

$$N = \frac{1}{2} \begin{pmatrix} 1 & -3 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix} \mathcal{A}(\text{tr}(A), \text{tr}(AB), \text{tr}(B)).$$

Moreover,

$$\nu = -1 \text{ for } \mathcal{A}(A, A^2B, AB)^{-1} \text{ and } \nu = 1 \text{ for } \mathcal{A}(AB, AB^2, B)^{-1}.$$

In other words, replacing A results in a positive value for ν , while replacing B results in a negative value for ν . Since $\text{tr}(AB) \geq \max(\text{tr}(A), \text{tr}(B))$ we can finally conclude that (6.29) implies a complete determination of the matrix $Z^{-1}\mathcal{A}$ in terms of Markoff triples and their affiliated quadratic residues subject to the specification (6.18).

6.9 Corollary The following identity holds true,

$$Z^{-1}\mathcal{A} = \begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix}^{-1} \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

7 Some number theoretic conclusions

The point of departure in the present section is the observation that, disregarding the factor $\frac{1}{2}$, on the one hand, the entries in the rows of the matrix on the right hand side of the identity (6.26) are the coefficients of indefinite binary quadratic forms which are equivalent to Markoff forms associated with the corresponding Markoff numbers in the last column, and which in the case of the last row corresponds to a reduced form, i.e. it actually is a Markoff form. On the other hand, the entries of the columns of the matrix on the left hand side are representations of the number 1 by the ternary quadratic form

$$(7.1) \quad Q(x, y, z) = xz - y^2$$

All elements in the group of automorphs of this form are given by the matrices

$$(7.2) \quad \begin{pmatrix} p^2 & 2pq & q^2 \\ pr & ps + qr & qs \\ r^2 & 2rs & s^2 \end{pmatrix}, \text{ where } \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{SL}(2, \mathbb{Z}).$$

This observation goes all the way back to Gauss (cf. [Ba], Kapitel I, pp. 22-23). If p, q, r, s are elements in an arbitrary commutative ring, then we always have the formula

$$\det \begin{pmatrix} p^2 & 2pq & q^2 \\ pr & ps + qr & qs \\ r^2 & 2rs & s^2 \end{pmatrix} = \left(\det \begin{pmatrix} p & q \\ r & s \end{pmatrix} \right)^3$$

For a given matrix $A \in \text{SL}(2, \mathbb{Z})$ let $\Psi(A)$ be the corresponding 3x3 matrix in (7.2). Then Ψ determines an isomorphism from the group $\text{PSL}(2, \mathbb{Z})$ onto the group of automorphs of the form (7.1) with determinant 1. For any integral solution of the equation

$$(7.3) \quad xz - y^2 = 1,$$

we define the number $|y|$ as the height of the triple (x, y, z) . Implementing a procedure akin to the continued fraction algorithm, it is an elementary task to show that, by employing a finite sequence of matrices of the form

$$\Psi \left(\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \right) \text{ and } \Psi \left(\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \right)$$

to a triple (x, y, z) , solving (7.3), one can reduce the height of such a triple to the smallest possible value, which is 0. In the sequel we shall need the following by-product of this procedure.

7.1 Lemma If (x, y, z) is a solution of (7.3), then the application of a matrix of the form

$\Psi\left(\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}\right)$ or $\Psi\left(\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}\right)$ to the vector $(x, y, z)^t$ does not change the sign of x and z .

Proof It suffices to note that the extreme value of the quadratic polynomial $xr^2 + 2yr + z$ is equal to $\frac{1}{x}$, while the extreme value of the quadratic polynomial $zq^2 + 2yq + x$ is equal to $\frac{1}{z}$. \square

An alternative way of looking at this situation is as follows. For any triple (x, y, z) consider the binary quadratic form $Q(s, t) = xs^2 + 2yst + zt^2$. Then the triple (x, y, z) solves the equation (7.3) if and only if the corresponding quadratic form Q is positive definite and has a discriminant which is equal to -4 . And so the argument just made turns out to be equivalent to the longstanding wisdom that all quadratic forms with this property are equivalent. Now let $A \in \text{SL}(2, \mathbb{Z})$ be such that

$$\Psi(A) \begin{pmatrix} \mathfrak{m} \\ k_m \\ l_m \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Remark The existence of such a matrix A can also be established through an application of part c) in Lemma 4.2.

It is not imperative to choose the second column of the matrix $\begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix}$.

The discussion

in the present section could be based on the other two choices as well. The expediency of choosing the second column will become clear in Section 10, however. If we write

$$\Psi(A) \begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix} = \begin{pmatrix} x_1 & 1 & x_2 \\ y_1 & 0 & y_2 \\ z_1 & 1 & z_2 \end{pmatrix}; x_i, y_i, z_i \in \mathbb{Z}; i \in \{1, 2\},$$

then,

(7.4)

$$\begin{pmatrix} x_1 & 1 & x_2 \\ y_1 & 0 & y_2 \\ z_1 & 1 & z_2 \end{pmatrix} \text{adj} = \begin{pmatrix} -y_2 & x_2 - z_2 & y_2 \\ y_2 z_1 - y_1 z_2 & x_1 z_2 - x_2 z_1 & x_2 y_1 - x_1 y_2 \\ y_1 & z_1 - x_1 & -y_1 \end{pmatrix},$$

and by (6.26)

(7.5)

$$\begin{pmatrix} x_1 & 1 & x_2 \\ y_1 & 0 & y_2 \\ z_1 & 1 & z_2 \end{pmatrix} \text{adj} = \begin{pmatrix} l_c + 3k_c & -(2k_c + 3\mathfrak{c}) & \mathfrak{c} \\ -(l_b + 3\nu k_b) & 2k_b + 3\nu \mathfrak{b} & -\mathfrak{b} \\ l_a - 3k_a & -(2k_a - 3\mathfrak{a}) & \mathfrak{a} \end{pmatrix} \Psi(A)^{-1}$$

Since an application from the left of the matrix $\Psi(A)^{-1}$ to a row vector corresponds to the transformation of the affiliated binary quadratic form by the matrix A^{-1} , and since the first and the third row of the matrix on the right hand side of (7.4) correspond to symmetric forms, we conclude that the quadratic forms corresponding to the first and the third row of the matrix

$$\begin{pmatrix} l_c + 3k_c & -(2k_c + 3\mathfrak{c}) & \mathfrak{c} \\ -(l_b + 3\nu k_b) & 2k_b + 3\nu \mathfrak{b} & -\mathfrak{b} \\ l_a - 3k_a & -(2k_a - 3\mathfrak{a}) & \mathfrak{a} \end{pmatrix} \text{ are equivalent to a symmetric form each.}$$

This leads to the

following significant conclusion.

7.2 Proposition Every cycle of reduced binary quadratic forms including a Markoff form also includes a symmetric form.

It has been known for a long time that every Markoff form F is equivalent to $-F$. Since a symmetric form H is obviously equivalent to $-F$, that statement follows immediately from Proposition 7.2. We turn now to the second row of the matrix on the right hand side of (7.4). First we note that,

(7.6)

$$\begin{aligned} \text{entry}(2, 1) + \text{entry}(2, 3) &= (y_2 z_1 - y_1 z_2) + (x_2 y_1 - x_1 y_2) \\ &= \det \begin{pmatrix} x_1 & 1 & x_2 \\ y_1 & 0 & y_2 \\ z_1 & 1 & z_2 \end{pmatrix} = \det \begin{pmatrix} \mathfrak{c} & \mathfrak{m} & \mathfrak{a} \\ k_c & k_m & k_a \\ l_c & l_m & l_a \end{pmatrix} = 2 \end{aligned}$$

It follows from (7.4) and (7.5) that the discriminant of this row is equal to $9\mathfrak{b}^2 - 4$. Hence,

$$\begin{aligned} &(x_1 z_2 - x_2 z_1)^2 - 4(y_2 z_1 - y_1 z_2)(x_2 y_1 - x_1 y_2) \\ &= (x_1 z_2 - x_2 z_1)^2 - 4(y_2 z_1 - y_1 z_2)(2 - (y_2 z_1 - y_1 z_2)) \end{aligned}$$

$$= (x_1 z_2 - x_2 z_1)^2 + 4(y_2 z_1 - y_1 z_2 - 1)^2 - 4 = 9\mathfrak{b}^2 - 4,$$

which leads to

$$(7.7) \quad (x_1 z_2 - x_2 z_1)^2 + 4(y_2 z_1 - y_1 z_2 - 1)^2 = 9\mathfrak{b}^2.$$

Since the sum of two squares is divisible by 3 if and only if each summand shares this property, we conclude that

$$\mathfrak{p} = \frac{1}{3}(x_1 z_2 - x_2 z_1)\epsilon\mathbb{Z}, \mathfrak{q} = \frac{1}{3}(y_2 z_1 - y_1 z_2 - 1)\epsilon\mathbb{Z},$$

and after rewriting (7.7) as

$$(7.8) \quad \mathfrak{p}^2 + 4\mathfrak{q}^2 = \mathfrak{b}^2,$$

the standard parametrization for Pythagorean triples ensures the existence if two integers, \mathfrak{f} and \mathfrak{g} , such that

$$\mathfrak{p} = \mathfrak{f}^2 - \mathfrak{g}^2, \mathfrak{q} = \mathfrak{f}\mathfrak{g}, \mathfrak{b} = \mathfrak{f}^2 + \mathfrak{g}^2.$$

In conclusion, the second row vector of the matrix on the right hand side of (7.4) takes the form,

$$(7.9) \quad (y_2 z_1 - y_1 z_2, x_1 z_2 - x_2 z_1, x_2 y_1 - x_1 y_2) = (1 + 3\mathfrak{f}\mathfrak{g}, 3(\mathfrak{f}^2 - \mathfrak{g}^2), 1 - 3\mathfrak{f}\mathfrak{g}).$$

To summarize, we have arrived at the following situation. Given a Markoff number \mathfrak{m} , there exist three equivalent quadratic forms,

$$(7.10) \quad \begin{aligned} F(s, t) &= \mathfrak{m}s^2 + (2k - 3\mathfrak{m})st + (l - 3k)t^2, k^2 + 1 = \mathfrak{m}l, 0 < 2k < \mathfrak{m} \\ G(s, t) &= (1 + 3\mathfrak{f}\mathfrak{g})s^2 + 3(\mathfrak{f}^2 - \mathfrak{g}^2)st + (1 - 3\mathfrak{f}\mathfrak{g})t^2, \\ H(s, t) &= \mathfrak{u}s^2 + \mathfrak{v}st - \mathfrak{u}t^2, \end{aligned}$$

all of which, after having been subjected to a transformation by the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, if necessary, may be assumed to be reduced. Standard theory for binary quadratic forms (cf. [L], Satz 202) ensures that there exist (fundamental) automorphs of these quadratic forms, which in each of these three particular cases take the form, in the order of their appearance above,

$$(7.11) \quad \begin{aligned} \mathfrak{F} &= \begin{pmatrix} 3\mathfrak{m} - k & 3k - l \\ \mathfrak{m} & k \end{pmatrix}, \\ \mathfrak{G} &= \begin{pmatrix} 3\mathfrak{g}^2 & 3\mathfrak{f}\mathfrak{g} - 1 \\ 3\mathfrak{f}\mathfrak{g} + 1 & 3\mathfrak{f}^2 \end{pmatrix}, \end{aligned}$$

$$\mathfrak{H} = \begin{pmatrix} \frac{3\mathfrak{m}-\mathfrak{v}}{2} & \mathfrak{u} \\ \mathfrak{u} & \frac{3\mathfrak{m}+\mathfrak{v}}{2} \end{pmatrix}.$$

Recall from [F], Gesammelte Abhandlungen, Band III, p.606 (IV) that a number \mathfrak{m} is Markoff if and only if \mathfrak{m} is representable by a quadratic form Q which is equivalent to $-Q$, and which has the discriminant $9\mathfrak{m}^2 - 4$. We can now give an alternative characterization of Markoff numbers.

7.3 Proposition An integer $\mathfrak{m} \geq 1$ is a Markoff number if and only if $\mathfrak{m} = \frac{1}{3} \text{tr}(\mathfrak{G})$, where

$\mathfrak{G} = \begin{pmatrix} 3\mathfrak{g}^2 & 3\mathfrak{f}\mathfrak{g} - 1 \\ 3\mathfrak{f}\mathfrak{g} + 1 & 3\mathfrak{f}^2 \end{pmatrix}$ for some integers $\mathfrak{f}, \mathfrak{g}$; and \mathfrak{G} is equivalent to a symmetric matrix.

Proof A unimodular 2x2 matrix which is equivalent to a symmetric matrix is also equivalent to A^t . But a matrix which conjugates A to A^t has to be symmetric too. This entails that A is the product of two symmetric matrices. Applied to a matrix of the form $\mathfrak{G} = \begin{pmatrix} 3\mathfrak{g}^2 & 3\mathfrak{f}\mathfrak{g} - 1 \\ 3\mathfrak{f}\mathfrak{g} + 1 & 3\mathfrak{f}^2 \end{pmatrix}$ which is unimodular for any \mathfrak{f} and \mathfrak{g} , this means that $\mathfrak{G} = \mathfrak{S}\mathfrak{T}$, where \mathfrak{S} and \mathfrak{T} are symmetric and unimodular. Since

$$(\mathfrak{S}\mathfrak{T})^t = \mathfrak{T}\mathfrak{S} = \begin{pmatrix} 3\mathfrak{g}^2 & 3\mathfrak{f}\mathfrak{g} - 1 \\ 3\mathfrak{f}\mathfrak{g} + 1 & 3\mathfrak{f}^2 \end{pmatrix},$$

and hence

$$\mathfrak{S}^{-1}\mathfrak{T}^{-1} = \begin{pmatrix} 3\mathfrak{f}^2 & -3\mathfrak{f}\mathfrak{g} - 1 \\ -3\mathfrak{f}\mathfrak{g} + 1 & 3\mathfrak{g}^2 \end{pmatrix},$$

we get

$$\mathfrak{S}\mathfrak{T}\mathfrak{S}^{-1}\mathfrak{T}^{-1} = \begin{pmatrix} 3\mathfrak{g}^2 & 3\mathfrak{f}\mathfrak{g} - 1 \\ 3\mathfrak{f}\mathfrak{g} + 1 & 3\mathfrak{f}^2 \end{pmatrix} \begin{pmatrix} 3\mathfrak{f}^2 & -3\mathfrak{f}\mathfrak{g} - 1 \\ -3\mathfrak{f}\mathfrak{g} + 1 & 3\mathfrak{g}^2 \end{pmatrix} = \begin{pmatrix} 6\mathfrak{f}\mathfrak{g} - 1 & -6\mathfrak{g}^2 \\ 6\mathfrak{f}^2 & -6\mathfrak{f}\mathfrak{g} - 1 \end{pmatrix}.$$

Hence $\text{tr}(\mathfrak{S}\mathfrak{T}\mathfrak{S}^{-1}\mathfrak{T}^{-1}) = -2$. Now Fricke's identity implies,

$$9\mathfrak{m}^2 + (\text{tr}(\mathfrak{S}))^2 + (\text{tr}(\mathfrak{T}))^2 = 3\mathfrak{m} \text{tr}(\mathfrak{S}) \text{tr}(\mathfrak{T}),$$

which means that \mathfrak{m} has to be a Markoff number. Thus we have shown that the enunciated condition is sufficient. That it is also necessary was shown above. \square

Proposition 7.2 in combination with the special form of the discriminant allows us to give a more incisive characterization of the cycles of reduced forms containing a Markoff form.

7.4 Proposition Any cycle of reduced forms containing a Markoff form associated with a Markoff number $\mathfrak{m} \geq 5$ contains two symmetric forms $H_1(s, t) = \mathfrak{u}_1 s^2 + \mathfrak{v}_1 st - \mathfrak{u}_1 t^2$ and $H_2(s, t) = \mathfrak{u}_2 s^2 + \mathfrak{v}_2 st - \mathfrak{u}_2 t^2$ such that $\mathfrak{u}_1 \neq -\mathfrak{u}_2$.

Proof By Proposition 7.2, any cycle of reduced forms containing a Markoff form F with discriminant $9\mathfrak{m}^2 - 4$ contains a symmetric form H with a fundamental automorph

$$\mathfrak{H} = \begin{pmatrix} \frac{3\mathfrak{m}-\mathfrak{v}}{2} & \mathfrak{u} \\ \mathfrak{u} & \frac{3\mathfrak{m}+\mathfrak{v}}{2} \end{pmatrix},$$

where

$$(7.12) \quad 4\mathfrak{u}^2 + \mathfrak{v}^2 = 9\mathfrak{m}^2 - 4.$$

First we deal with the case when \mathfrak{m} is odd. Employing the standard parametrization for Pythagorean quadruples (cf. [M2], p.14) we conclude that there exist integers n, p, q, r such that

$$(7.13) \quad \begin{aligned} 1 &= nr - pq, \mathfrak{u} = nq + pr, \\ \mathfrak{v} &= -n^2 - p^2 + q^2 + r^2, 3\mathfrak{m} = n^2 + p^2 + q^2 + r^2. \end{aligned}$$

Hence,

$$(7.14) \quad \mathfrak{T}\mathfrak{T}^t = \mathfrak{H}, \text{ where } \mathfrak{T} = \begin{pmatrix} n & p \\ q & r \end{pmatrix}, \det(\mathfrak{T}) = 1$$

We claim that $n \neq r$. Suppose this were not true. Then,

$$\mathfrak{u} = n(q + p), \mathfrak{v} = (q + p)(q - p).$$

It follows from (7.12)

$$(7.15) \quad q + p \text{ divides the discriminant } 9\mathfrak{m}^2 - 4.$$

Moreover, since the three coefficients of H are divisible by $q + p$, every integer represented by H is divisible by $q + p$. Since H and F are equivalent, and since \mathfrak{m} is represented by F , \mathfrak{m} is represented by H as well. It follows that \mathfrak{m} is divisible by $q + p$. Combined with (7.15) this implies that $q + p$ is odd and that 4 is divisible by $q + p$. Hence,

$$(7.16) \quad q + p = 1 \text{ or } q + p = -1$$

Combining the first identity in (7.16) with the first identity in (7.13) yields,

$$(7.17) \quad n^2 + p^2 = 1 + p.$$

This diophantine equation has four solutions, namely $(n, p) = (\pm 1, 0)$ and $(n, p) = (\pm 1, 1)$. Combining the second identity in (7.16) with the first identity in (7.13) yields,

(7.18)

$$n^2 + p^2 = 1 - p.$$

This diophantine equation has four solutions, namely $(n, p) = (\pm 1, -1)$ and $(n, p) = (\pm 1, 0)$. In conclusion, for all solutions of (7.17) and (7.18) we get $4\mathfrak{u}^2 + \mathfrak{v}^2 = 5$, which implies $\mathfrak{m} = 1$, and therefore $n \neq r$ as claimed, in case \mathfrak{m} is odd and $\mathfrak{m} \geq 5$.

We turn to the case of an even Markoff number \mathfrak{m} . In this case (7.12) implies that \mathfrak{v} is even. Letting $\mathfrak{w} = \frac{\mathfrak{v}}{2}$, (7.12) turns into

(7.19)

$$\mathfrak{u}^2 + \mathfrak{w}^2 = 9\mathfrak{m}^2 - 1.$$

But this implies that \mathfrak{u} and \mathfrak{w} have to be even. Hence, letting $\mathfrak{u} = \frac{\mathfrak{u}}{2}, \mathfrak{w} = \frac{\mathfrak{w}}{2}$, (7.19) turns into

(7.20)

$$(2\mathfrak{u})^2 + (2\mathfrak{w})^2 = 9\mathfrak{m}^2 - 1.$$

This time the parametrization takes the following form. There exist integers n, p, q, r , such that

(7.21)

$$\begin{aligned} \mathfrak{u} &= nr - pq, \mathfrak{v} = nq + pr, \\ 1 &= n^2 + p^2 - q^2 - r^2, 3\mathfrak{m} = n^2 + p^2 + q^2 + r^2. \end{aligned}$$

Hence,

(7.22)

$$\mathfrak{T}\mathfrak{T}^t = \mathfrak{H}, \text{ where } \mathfrak{T} = \begin{pmatrix} n - q & r - p \\ r + p & n + q \end{pmatrix}, \det(\mathfrak{T}) = 1.$$

We claim that $n - q \neq n + q$. Suppose this were not true. Then $q = 0$, and therefore,

(7.23)

$$\mathfrak{u} = nr, \mathfrak{v} = pr.$$

It follows from (7.12),

(7.24)

$$r \text{ divides the discriminant } 9\mathfrak{m}^2 - 4.$$

Moreover, since the three coefficients of H are divisible by r , every integer represented by H is divisible by r . Since H and F are equivalent, and since \mathfrak{m} is represented by F , \mathfrak{m} is represented by H as well. It follows that \mathfrak{m} is divisible by r . Combined with (7.20) this implies that that 2 is divisible by r . If $|r| = 2$, then the third identity in (7.21) yields $n^2 + p^2 = 5$. Substituting this into the fourth identity in (7.21) leads to $\mathfrak{m} = 3$, hence to $\mathfrak{m} = 6$, which is not a Markoff number. If $|r| = 1$, then the third identity in (7.21) implies that $n^2 + p^2 = 2$. Substituting this into the fourth identity in (7.21) leads to $\mathfrak{m} = 1$, hence to

$\mathfrak{m} = 2$. In conclusion, $n - q \neq n + q$ as claimed, in case $\mathfrak{m} \geq 5$ is an even Markoff number.

Combining the two separate cases for \mathfrak{m} , we have shown that there always exists a matrix $\mathfrak{T} \in \mathrm{SL}(2, \mathbb{Z})$ with distinct diagonal entries such that $\mathfrak{T}\mathfrak{T}^t = \mathfrak{H}$. Considering such a matrix \mathfrak{T}_1 for \mathfrak{H}_1 , let $\mathfrak{H}_2 = \mathfrak{T}_1^t \mathfrak{T}_1$. Then,

$$\mathfrak{H}_2 = \mathfrak{T}_1^{-1} \mathfrak{H}_1 \mathfrak{T}_1.$$

Thus, \mathfrak{H}_2 is a fundamental automorph for a symmetric form H_2 which is equivalent to H_1 . Since the diagonal entries of \mathfrak{H}_1 are distinct, the sum of the first coefficient of H_1 and H_2 can not be zero \square

Remarks 1) In case $\mathfrak{m} = 1$ and $\mathfrak{m} = 2$ the (reduced) Markoff form is symmetric and ambiguous.

2) Proposition 7.4 places all cycles of reduced forms which include Markoff forms with a discriminant larger than 32 among the so-called ambiguous cycles. In terms of the classification scheme of cycles exhibited in [Bu], pp. 28-29, the cycles containing two “non-affiliated” symmetric forms are being addressed as “Type 20”. It follows in particular that a Markoff form with a discriminant larger than 32 can never be equivalent to an ambiguous form. For more information about the computational aspects of ambiguous cycles see [BV], 6.14

3) Any unimodular integral matrix of the form $\mathfrak{F} = \begin{pmatrix} 3\mathfrak{m} - k & 3k - l \\ \mathfrak{m} & k \end{pmatrix}$, \mathfrak{m} being a positive integer, is equivalent to a matrix of the form $\mathfrak{G} = \begin{pmatrix} 3\mathfrak{g}^2 & 3\mathfrak{f}\mathfrak{g} - 1 \\ 3\mathfrak{f}\mathfrak{g} + 1 & 3\mathfrak{f}^2 \end{pmatrix}$.

To see this we note that the unimodularity of \mathfrak{F} implies the unimodularity of the matrix $\mathfrak{S} = \begin{pmatrix} \mathfrak{m} & k \\ k & l \end{pmatrix}$. Hence, by Lemma 4.2 part c) there exists a matrix $\mathfrak{T} \in \mathrm{SL}(2, \mathbb{Z})$, such that $\mathfrak{S} = \mathfrak{T}\mathfrak{T}^t$. It is now an elementary task to check that $\mathfrak{T}\mathfrak{F}\mathfrak{T}^{-1} = \mathfrak{G}$.

4) The matrix on the right hand side of the identity (7.5) can be written as follows,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \mathfrak{c} & \mathfrak{b} & \mathfrak{a} \\ k_c + 3\mathfrak{c} & k_b & k_a \\ l_c + 6k_c + 9\mathfrak{c} & l_b & l_a \end{pmatrix}^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -3 & 1 \\ -3 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix} \Psi(A)^{-1},$$

in case $\nu = -1$ and

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \mathfrak{c} & \mathfrak{b} & \mathfrak{a} \\ k_c + 3\mathfrak{c} & k_b + 3\mathfrak{b} & k_a \\ l_c + 6k_c + 9\mathfrak{c} & l_b + 6k_b + 9\mathfrak{b} & l_a \end{pmatrix}^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -3 & 1 \\ -3 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix} \Psi(A)^{-1},$$

in case $\nu = -1$ and

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \mathfrak{c} & \mathfrak{b} & \mathfrak{a} \\ k_c + 3\mathfrak{c} & k_b + 3\mathfrak{b} & k_a \\ l_c + 6k_c + 9\mathfrak{c} & l_b + 6k_b + 9\mathfrak{b} & l_a \end{pmatrix}^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -3 & 1 \\ -3 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix} \Psi(A)^{-1},$$

in case $\nu = 1$. One can show that $\Psi(A)$ satisfies the identity

$$\begin{pmatrix} 0 & -3 & 1 \\ -3 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix} \Psi(A)^{-1} = (\Psi(A)^{-1})^t \begin{pmatrix} 0 & -3 & 1 \\ -3 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

if and only if A is of the form $\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$. It is this identity that explains why we are staying within the same equivalence class of quadratic residues on both sides of the identity (7.5), as long as we apply matrices of the form $\Psi\left(\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}\right)$ only. That fact was implicitly instrumental in the proof of Proposition 6.1.

We are now going to refine the analysis of the matrix in (7.4). Since $\Psi(A)$ is an automorph of the quadratic form Q , we get,

$$(7.25) \quad y_i^2 + 1 = x_i z_i, i \in \{1, 2\}.$$

Since the first row of the matrix in (7.5) has the discriminant $9\mathfrak{c}^2 - 4$, while the third row has the discriminant $9\mathfrak{a}^2 - 4$, we also get,

$$(7.26) \quad (x_1 - z_1)^2 + 4y_2^2 = 9\mathfrak{a}^2 - 4, \quad (x_2 - z_2)^2 + 4y_2^2 = 9\mathfrak{c}^2 - 4 \quad .$$

Combining (7.25) and (7.26) for $i = 1$ and $i = 2$, respectively, leads to,

$$(x_1 + z_1)^2 = 9\mathfrak{a}^2, (x_2 + z_2)^2 = 9\mathfrak{c}^2.$$

By Lemma 7.1

$$(7.27) \quad x_1 + z_1 = 3\mathfrak{a}, x_2 + z_2 = 3\mathfrak{c},$$

Letting

$$v_a = x_1 - z_1, v_c = x_2 - z_2$$

we can recast the identities (7.27) as follows,

$$(7.28) \quad x_1 = \frac{1}{2}(3\mathfrak{a} + v_a), z_1 = \frac{1}{2}(3\mathfrak{a} - v_a), x_2 = \frac{1}{2}(3\mathfrak{c} + v_c), z_2 = \frac{1}{2}(3\mathfrak{c} - v_c).$$

Substituting these expressions into the second row of the matrix in (7.4), and combining the result with (7.8) yields,

(7.29)

$$\begin{pmatrix} \frac{1}{2}y_2(3\mathfrak{a} - v_a) - \frac{1}{2}y_1(3\mathfrak{c} - v_c) \\ \frac{1}{4}(3\mathfrak{a} + v_a)(3\mathfrak{c} - v_c) - \frac{1}{4}(3\mathfrak{c} + v_c)(3\mathfrak{a} - v_a) \\ \frac{1}{2}y_1(3\mathfrak{c} + v_c) - \frac{1}{2}y_2(3\mathfrak{a} + v_a) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} y_2(3\mathfrak{a} - v_a) - y_1(3\mathfrak{c} - v_c) \\ 3(\mathfrak{c}v_a - \mathfrak{a}v_c) \\ y_1(3\mathfrak{c} + v_c) - y_2(3\mathfrak{a} + v_a) \end{pmatrix}$$

$$= \begin{pmatrix} 1 + 3\mathfrak{f}\mathfrak{g} \\ 3(\mathfrak{f}^2 - \mathfrak{g}^2) \\ 1 - 3\mathfrak{f}\mathfrak{g} \end{pmatrix} = \begin{pmatrix} 1 + 3\mathfrak{q} \\ 3\mathfrak{p} \\ 1 - 3\mathfrak{q} \end{pmatrix}.$$

Writing the identities for the first and the third component as a linear system in y_1 and y_2 , and then solving for these two parameters leads to,

$$3(\mathfrak{a}v_c - \mathfrak{c}v_a) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3\mathfrak{a} + v_a & 3\mathfrak{a} - v_a \\ 3\mathfrak{c} + v_c & 3\mathfrak{c} - v_c \end{pmatrix} \begin{pmatrix} 1 + 3\mathfrak{q} \\ 1 - 3\mathfrak{q} \end{pmatrix} = 6 \begin{pmatrix} \mathfrak{q}v_a + \mathfrak{a} \\ \mathfrak{q}v_c + \mathfrak{c} \end{pmatrix},$$

and finally, after invoking the second component identity in (7.29), letting $u_a = y_1, u_c = y_2$,

(7.30)

$$\mathfrak{p}u_a + \mathfrak{q}v_a = -\mathfrak{a}, \mathfrak{p}u_c + \mathfrak{q}v_c = -\mathfrak{c}.$$

In conclusion, we have shown the following.

7.5 Proposition Given a Markoff number \mathfrak{b} , and any Markoff number \mathfrak{a} such that \mathfrak{a} and \mathfrak{b} belong to a common triple of Markoff numbers, the system of diophantine equations

(7.31)

$$p^2 + q^2 = \mathfrak{b}^2, u^2 + v^2 = 9\mathfrak{a}^2 - 4, pu + qv = -2\mathfrak{a},$$

is always solvable. Moreover, the decomposition of \mathfrak{b} into a sum of two squares which is obtained from the first equation through the standard parametrization for Pythagorean triples, and the decomposition of the discriminant $9\mathfrak{a}^2 - 4$ into a sum of two squares in the second equation, are uniquely determined by these three equations. The former is affiliated with the quadratic residue k_b of -1 modulo \mathfrak{b} .

We have yet to address the uniqueness part in this statement. To do so, we express the three identities in (7.31) in matrix form,

(7.32)

$$\begin{pmatrix} p & q \\ u & v \end{pmatrix} \begin{pmatrix} p & q \\ u & v \end{pmatrix}^t = \begin{pmatrix} p & q \\ u & v \end{pmatrix} \begin{pmatrix} p & u \\ q & v \end{pmatrix} = \begin{pmatrix} \mathfrak{b}^2 & -2\mathfrak{a} \\ -2\mathfrak{a} & 9\mathfrak{a}^2 - 4 \end{pmatrix},$$

and note that the matrix $\begin{pmatrix} p & q \\ u & v \end{pmatrix}$ is uniquely determined up to multiplication from the right by an orthogonal integral matrix. Going one step further

we note that,

$$\det \begin{pmatrix} \mathfrak{b}^2 & -2\mathfrak{a} \\ -2\mathfrak{a} & 9\mathfrak{a}^2 - 4 \end{pmatrix} = \frac{1}{9}((9\mathfrak{a}^2 - 4)(9\mathfrak{b}^2 - 4) - 16) = (3\mathfrak{a}\mathfrak{b} + 2\mathfrak{c})^2$$

is a perfect square. Since the entries of this matrix are relatively prime, a theorem by L. Mordell ([M1], [Ni]) on the decomposition of a binary quadratic form into a sum of the square of two linear forms is applicable, yielding an independent proof for the existence of a matrix $\begin{pmatrix} p & q \\ u & v \end{pmatrix}$ which satisfies the identity (7.32). This argument, however, does not provide any information regarding the last statement in Proposition 7.5. If \mathfrak{b} is prime, then the validity of that claim is obvious. If \mathfrak{b} is not prime, then there is an issue, which was addressed in Remark 3 above.

8. Markoff triples and the norm form equation

Having established the uniqueness of a dominant Markoff number in Section 5, there are two aspects that will be touched upon in the remainder of this work. First, a description of the data that are being determined by a single Markoff number \mathfrak{m} in a way that reflects its dominance, and second, in consideration of the multitude of identities that led to the conclusion of the uniqueness of a dominant Markoff number, to highlight the purely algebraic side of the formalism. To deal with the former, we shall adopt as a framework a norm form equation that uses no data other than \mathfrak{m} and the discriminant $9\mathfrak{m}^2 - 4$. To appreciate the need for the latter, it suffices to point out, that for any pair of non-zero rational numbers u and v the triple (a, b, c) of rational numbers, where

$$a = \frac{u^2 + v^2 + 1}{u}, b = \frac{u^2 + v^2 + 1}{u}, c = \frac{u^2 + v^2 + 1}{uv},$$

solves the Markoff equation $a^2 + b^2 + c^2 = abc$, a fact that hints at a lack of depth of the whole formalism when considered within this broader setting. The two aspects turn out to be linked to each other in some way. To begin with, we need to introduce the necessary framework for the discussion and switch to a more expedient notation. Let $(\mathfrak{m}, \mathfrak{a}_0, \mathfrak{a}_1)$ be a Markoff triple such that $\mathfrak{m} \geq \mathfrak{a}_1 \geq \mathfrak{a}_0$, and define recursively

$$(8.1) \quad \mathfrak{a}_{n+1} = 3\mathfrak{m}\mathfrak{a}_n - \mathfrak{a}_{n-1} \text{ for } n \geq 1, \mathfrak{a}_{n-1} = 3\mathfrak{m}\mathfrak{a}_n - \mathfrak{a}_{n+1} \text{ for } n \leq 0$$

Then the uniqueness of the dominant Markoff number \mathfrak{m} implies that, up to permutations, the two-sided sequence of triples $(\mathfrak{m}, \mathfrak{a}_n, \mathfrak{a}_{n+1}), n \in \mathbb{Z}$, represents exactly all those Markoff triples which contain \mathfrak{m} as a member. Notice, however,

that in case $\mathfrak{m} = 1$ or $\mathfrak{m} = 2$ the recursion is essentially only one-sided, leading to a duplication of Markoff numbers if the recursion is two-sided. Let λ be the following fundamental unit and its inverse, respectively, in the quadratic field $\mathbb{Q}(\sqrt{9\mathfrak{m}^2 - 4})$,

$$(8.2) \quad \lambda = \frac{3\mathfrak{m}}{2} + \frac{\sqrt{9\mathfrak{m}^2 - 4}}{2}, \lambda^{-1} = \frac{3\mathfrak{m}}{2} - \frac{\sqrt{9\mathfrak{m}^2 - 4}}{2}$$

For $x = r + s\sqrt{9\mathfrak{m}^2 - 4}$ ($r, s \in \mathbb{Q}$) in $\mathbb{Q}(\sqrt{9\mathfrak{m}^2 - 4})$ we denote by $x^* = r - s\sqrt{9\mathfrak{m}^2 - 4}$ its conjugate. Let

$$(8.3) \quad \omega = \frac{\mathfrak{a}_1 - \mathfrak{a}_0\lambda^{-1}}{\sqrt{9\mathfrak{m}^2 - 4}} = \frac{\mathfrak{a}_0}{2} + \frac{3\mathfrak{a}_0\mathfrak{m} - 2\mathfrak{a}_1}{2\sqrt{9\mathfrak{m}^2 - 4}}.$$

Then

$$(8.4) \quad \mathfrak{a}_n = \omega\lambda^n + \omega^*\lambda^{-n} \text{ for all } n \in \mathbb{Z},$$

and $\omega\omega^*$ solves the norm form equation,

$$(8.5) \quad (9\mathfrak{m}^2 - 4)\omega\omega^* = \mathfrak{m}^2,$$

or, written as a diophantine equation,

$$(8.6) \quad x^2 - Dy^2 = -4\mathfrak{m}^2, \text{ where } D = 9\mathfrak{m}^2 - 4,$$

where,

$$(8.7) \quad x = 3\mathfrak{a}_0\mathfrak{m} - 2\mathfrak{a}_1, y = \mathfrak{a}_1.$$

A solution $(x, y) = (u, v)$ of the norm form equation (8.6) is called a fundamental solution ([St]), if the following two inequalities hold,

$$(8.8) \quad 0 < v \leq \frac{\mathfrak{m}}{\sqrt{3\mathfrak{m} - 2}}, \quad |u| \leq \mathfrak{m}\sqrt{3\mathfrak{m} - 2}.$$

For any solution (x, y) of (8.6) there exists a fundamental solution (u, v) and an integer n such that

$$x + y\sqrt{D} = (u + v\sqrt{D})\lambda^n,$$

and two solutions for which such a relation holds with a common fundamental solution $u + v\sqrt{D}$ are called equivalent. In the general theory of norm form equations it is shown, that the first equation in (8.6), with more general parameters on either side of the equation, has only finitely many fundamental solutions. The solution (8.7) is a fundamental solution. Since $\mathfrak{a}_1 \geq \mathfrak{a}_0$ by assumption, the first inequality in (8.8) trivially implies the second one. Switching the roles

of \mathfrak{a}_0 and \mathfrak{a}_1 leads to the conjugate equivalence class of solutions, which in this particular case is always distinct from the former in case $\mathfrak{m} \geq 5$. The uniqueness of the dominant Markoff number \mathfrak{m} is equivalent to the statement that there are no other other equivalence classes of solutions.

9 Recursions for the discriminant

We return now to the settings of Proposition 7.5, while retaining the notation in (8.1) for Markoff numbers which belong to a triple that includes \mathfrak{m} , to show that the three diophantine equations in (7.31) fit the scheme of a recursion akin to the one in (8.1). By Proposition 7.5 there exist four integers u_0, u_1, v_0, v_1 such that

$$(9.1) \quad u_n^2 + v_n^2 = 9\mathfrak{a}_n^2 - 4$$

$$(9.2) \quad \mathfrak{p}u_n + \mathfrak{q}v_n = -2\mathfrak{a}_n,$$

for $n \in \{0, 1\}$, and

$$(9.3) \quad \mathfrak{p}^2 + \mathfrak{q}^2 = \mathfrak{m}^2.$$

The second component identity in (7.29) yields,

$$(9.4) \quad \mathfrak{a}_1 v_0 - \mathfrak{a}_0 v_1 = 2\mathfrak{p}.$$

Moreover, the Pythagorean triple $(\mathfrak{m}, \mathfrak{p}, \mathfrak{q})$ is (uniquely) affiliated with the residue classes

$$\pm \frac{\mathfrak{a}_0}{\mathfrak{a}_1} \text{ modulo } \mathfrak{m}.$$

By Proposition 7.4 and the second component identity in (7.29) there exist integers $\mathfrak{u}_1, \mathfrak{u}_2, \mathfrak{v}_1, \mathfrak{v}_2$ such that

$$(9.5) \quad \mathfrak{u}_i^2 + \mathfrak{v}_i^2 = 9\mathfrak{a}_i^2 - 4, \mathfrak{p}\mathfrak{u}_i + \mathfrak{q}\mathfrak{v}_i = -2\mathfrak{a}_i, i \in \{1, 2\}; \mathfrak{a}_2 \mathfrak{v}_1 - \mathfrak{a}_1 \mathfrak{v}_2 = 2\mathfrak{p}.$$

9.1 Lemma The following identities hold true,

$$(9.6) \quad \mathfrak{u}_2 = 3\mathfrak{m}u_1 - u_0, \mathfrak{v}_2 = 3\mathfrak{m}v_1 - v_0.$$

Proof Let $u_2 = 3mu_1 - u_0$, $v_2 = 3mv_1 - v_0$. Then

$$pu_2 + qv_2 = p(3mu_1 - u_0) + q(3mv_1 - v_0) = 3m(pu_1 + qv_1) - (pu_0 + qv_0) = -2(3ma_1 - a_0) = -2a_2.$$

It follows from this and the second identity in (9.5) for $i = 2$ that there exists an integer x such that $v_2 = v_1 + px$, and it follows from (9.2) for $n = 1$ as well as the second identity in (9.5) for $i = 1$, that there exists an integer y such that $v_1 = v_0 + py$. The third identity in (9.5) and (9.4), together with (8.1) yield,

$$\begin{aligned} a_2v_1 - a_1v_2 &= a_2(v_0 + py) - a_1(v_1 + px) = a_2v_0 + a_2py - a_1v_1 - a_1px \\ &= (a_2 - 3ma_1)v_0 + a_1v_1 + (a_2y - a_1x)p = -a_0v_0 + a_1v_1 + (a_2y - a_1x)p = 2p + (a_2y - a_1x)p = 2p. \end{aligned}$$

It follows that $a_2y - a_1x = 0$. Hence, since a_1 and a_2 are relatively prime, a_2 divides x , and a_1 divides y . Now suppose that x , and hence y are non-zero. Then, by (9.1) for $i = 1$, and by the first identity in (9.5),

$$pa_1 \leq |v_1 - v_0| \leq \max(|v_1|, |v_0|) \leq \sqrt{9a_1^2 - 4} < 3a_1.$$

This implies that $p \leq 2$, and hence either $p = 1$ or $p = 2$. If $p = 1$, then by (9.3), $m = 1$ and $q = 0$, which is impossible. If $p = 2$, then again by (9.3), either $m = 2$ and $q = 0$, or m is not an integer, which is also impossible. In conclusion $x = y = 0$, thus settling the claim. \square

Replacing $i \in \{1, 2\}$ in (9.5) by $i \in \{-1, 0\}$ and repeating the arguments in the proof of Lemma 9.1 yields the identities $u_{-1} = 3mu_0 - u_1$, $v_{-1} = 3mv_0 - v_1$. A simple induction argument that uses nothing but Lemma 9.1 and this modified version establishes the following.

9.2 Proposition There exist two uniquely determined two-sided sequences of integers $\{u_n\}$ and $\{v_n\}$ such that

$$\begin{aligned} u_{n+1} &= 3mu_n - u_{n-1}, v_{n+1} = 3mv_n - v_{n-1} \\ u_n^2 + v_n^2 &= 9a_n^2 - 4, pu_n + qv_n = -2a_n, \end{aligned}$$

Remark If

$$\mathcal{A}_n = \begin{pmatrix} 9a_{n+1}^2 - 4 & 9a_n a_{n+1} - 6m \\ 9a_n a_{n+1} - 6m & 9a_n^2 - 4 \end{pmatrix}, \quad n \in \mathbb{Z}; \quad \mathcal{B} = \begin{pmatrix} 3m & 1 \\ -1 & 0 \end{pmatrix},$$

then

$$\det(\mathcal{A}_n) = 16, \mathcal{B}^t \mathcal{A}_n \mathcal{B} = \begin{pmatrix} 9a_{n+2}^2 - 4 & 9a_{n+1} a_{n+2} - 6m \\ 9a_{n+1} a_{n+2} - 6m & 9a_{n+1}^2 - 4 \end{pmatrix}.$$

Since $\det(\mathcal{A}_n)$ is a perfect square, and since the greatest common divisor of the entries of \mathcal{A}_n is equal to 1, it follows from Mordell's theorem that there exists an integral 2x2 matrix \mathcal{C}_n such that

$$\det(\mathcal{C}_n) = 4, \mathcal{C}_n^t \mathcal{C}_n = \mathcal{A}.$$

Comparison with Proposition 9.2 yields the following identity

(9.7)

$$u_n v_n + u_{n+1} v_{n+1} = 9\mathfrak{a}_n \mathfrak{a}_{n+1} - 6\mathfrak{m},$$

which is of some interest in its own right.

10 Recursions for the quadratic residues

In this final section the algebraic framework for the recursions involving the parameters k and l will be sketched. The major purpose is to highlight the role of the matrix \mathfrak{F} in this context. Returning to the settings at the beginning of Section 7, especially (7.4) and (7.5), we will employ Proposition 9.2 to convert the recursions for the u_n and v_n into recursions for the quadratic residues. In order to remain consistent with the notation introduced in Section 7, the Markoff number around which the recursion is to be developped will be denoted by \mathfrak{b} rather than \mathfrak{m} . In the applications of the formalism of Section 9 the letter \mathfrak{m} has to be replaced throughout by the letter \mathfrak{b} . First, transcribing (8.1), the point of departure are the recursions for all Markoff triples which include \mathfrak{b} ,

(10.1)

$$\mathfrak{a}_{n+1} = 3\mathfrak{b}\mathfrak{a}_n - \mathfrak{a}_{n-1} \text{ for } n \geq 1, \mathfrak{a}_{n-1} = 3\mathfrak{b}\mathfrak{a}_n - \mathfrak{a}_{n+1} \text{ for } n \leq 0.$$

under the proviso that,

(10.2)

$$\mathfrak{b} \geq \max(\mathfrak{a}_{-1}, \mathfrak{a}_0).$$

This implies that for some $\omega \in \mathbb{Q}(\sqrt{9\mathfrak{b}^2 - 4})$ we have $\mathfrak{a}_n = \omega \lambda^n + \omega^* \lambda^{-n}$ for all $n \in \mathbb{Z}$. Next, we need to adapt the identity (6.26) for our current needs. Since the parameter ν is going to change to its opposite sign as we pass through the triple which \mathfrak{b} dominates in the recursion (10.1), we define a one-sided recursion, Opting for $\nu = -1$, we note that the case for $\nu = 1$ can be handled in a similar way. Thus the identity (6.26) for values of $n \geq 1$ takes the form

(10.3)

$$\begin{pmatrix} \mathfrak{a}_{n-1} & \mathfrak{m}_n & \mathfrak{a}_n \\ k_{n-1} & \mathbb{k}_n & k_n \\ l_{n-1} & \mathbb{l}_n & l_n \end{pmatrix}^{-1} = \frac{1}{2} \begin{pmatrix} l_{n-1} + 3k_{n-1} & -(2k_{n-1} + 3\mathfrak{c}_{n-1}) & \mathfrak{a}_{n-1} \\ -(l_b - 3k_b) & 2k_b - 3\mathfrak{b} & -\mathfrak{b} \\ l_n - 3k_n & -(2k_n - 3\mathfrak{a}_n) & \mathfrak{a}_n \end{pmatrix},$$

From Section 7, in particular (7.28) we know that for every n there exists $A_n \in \text{SL}(2, \mathbb{Z})$ such that

$$\begin{aligned} \Psi(A_n) \begin{pmatrix} \mathfrak{a}_{n-1} & \mathfrak{m}_n & \mathfrak{a}_n \\ k_{n-1} & \mathbb{k}_n & k_n \\ l_{n-1} & \mathbb{l}_n & l_n \end{pmatrix} &= \begin{pmatrix} \frac{1}{2}(3\mathfrak{a}_n + v_n) & 1 & \frac{1}{2}(3\mathfrak{a}_{n-1} + v_{n-1}) \\ u_n & 0 & u_{n-1} \\ \frac{1}{2}(3\mathfrak{a}_n - v_n) & 1 & \frac{1}{2}(3\mathfrak{a}_{n-1} - v_{n-1}) \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{2}(3\mathfrak{a}_1 + v_1) & 1 & \frac{1}{2}(3\mathfrak{a}_0 + v_0) \\ u_1 & 0 & u_0 \\ \frac{1}{2}(3\mathfrak{a}_1 - v_1) & 1 & \frac{1}{2}(3\mathfrak{a}_0 - v_0) \end{pmatrix} \begin{pmatrix} \mathfrak{b} & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}^{n-1} \\ &= \Psi(A_1) \begin{pmatrix} \mathfrak{a}_0 & \mathfrak{m}_1 & \mathfrak{a}_1 \\ k_0 & \mathbb{k}_1 & k_1 \\ l_0 & \mathbb{l}_1 & l_1 \end{pmatrix} \begin{pmatrix} 3\mathfrak{b} & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}^{n-1} \end{aligned}$$

Let $\mathcal{F}_n = \Psi(A_1)^{-1} \Psi(A_n)$, and let $\mathcal{B} = \begin{pmatrix} 3\mathfrak{b} & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$. Then for every $n \geq 1$,

$$\mathcal{F}_n \begin{pmatrix} \mathfrak{a}_{n-1} & \mathfrak{m}_n & \mathfrak{a}_n \\ k_{n-1} & \mathbb{k}_n & k_n \\ l_{n-1} & \mathbb{l}_n & l_n \end{pmatrix} = \begin{pmatrix} \mathfrak{a}_0 & \mathfrak{m}_1 & \mathfrak{a}_1 \\ k_0 & \mathbb{k}_1 & k_1 \\ l_0 & \mathbb{l}_1 & l_1 \end{pmatrix} \mathcal{B}^{n-1},$$

and (10.3) implies

$$\mathcal{F}_n^t \begin{pmatrix} l_b - 3k_b \\ 3\mathfrak{b} - 2k_b \\ \mathfrak{b} \end{pmatrix} = \begin{pmatrix} l_b - 3k_b \\ 3\mathfrak{b} - 2k_b \\ \mathfrak{b} \end{pmatrix}.$$

It follows that there exists an integer j_n such that

$$\mathcal{F}_n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 1 & 0 & 1 \end{pmatrix} \Psi(\mathfrak{F})^{j_n} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \mathfrak{F} = \begin{pmatrix} 3\mathfrak{m} - k & 3k - l \\ \mathfrak{m} & k \end{pmatrix}$$

Some further considerations show that $j_n = -n + 1$, and hence a closer look at the the structure of the following matrix is desirable,

(10.4)

$$\mathcal{F} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 1 & 0 & 1 \end{pmatrix} \Psi(\mathfrak{F}) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Let

(10.5)

$$\varrho_{\pm} = \frac{2k_b \pm 3\mathfrak{b}}{2\mathfrak{b}} + \frac{\sqrt{9\mathfrak{b}^2 - 4}}{2\mathfrak{b}}$$

The coefficients of the corresponding quadratic form F can be recovered from this quantity by noting,

(10.6)

$$\frac{\mathfrak{b}}{2}(\varrho_{\pm} + \varrho_{\pm}^*) = 2k_b \pm 3\mathfrak{b}, \mathfrak{b}\varrho_{\pm}\varrho_{\pm}^* = l_b \pm 3k_b$$

The diagonalization of the matrix \mathcal{F} is the content of the next statement.

10.1 Lemma The following identity holds true, letting $\varrho = \varrho_-$

(10.7)

$$\begin{aligned} & \frac{1}{(\varrho - \varrho^*)^2} \begin{pmatrix} (\varrho^*)^2 & -2\varrho^* & 1 \\ -2\varrho\varrho^* & 2(\varrho + \varrho^*) & -2 \\ \varrho^2 & -2\varrho & 1 \end{pmatrix} \mathcal{F} \begin{pmatrix} 1 & 1 & 1 \\ \varrho & \frac{1}{2}(\varrho + \varrho^*) & \varrho^* \\ \varrho^2 & \varrho\varrho^* & (\varrho^*)^2 \end{pmatrix} \\ & \frac{1}{\omega\omega^*} \begin{pmatrix} (\varrho^*)^2 & -2\varrho^* & 1 \\ -2\varrho\varrho^* & 2(\varrho + \varrho^*) & -2 \\ \varrho^2 & -2\varrho & 1 \end{pmatrix} \mathcal{F} \begin{pmatrix} 1 & 1 & 1 \\ \varrho & \frac{1}{2}(\varrho + \varrho^*) & \varrho^* \\ \varrho^2 & \varrho\varrho^* & (\varrho^*)^2 \end{pmatrix} = \begin{pmatrix} \lambda^2 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & \lambda^{-2} \end{pmatrix} \end{aligned}$$

The proof of Lemma 10.1 is obtained through manipulations involving the identities (10.6). At this point a comment about the general pattern of the eigenvalues of a matrix of the form $\Psi\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix}\right)$ is in order. The characteristic polynomial is always of the form

$$-x^3 + (\mathfrak{t}^2 - 1)x^2 - (\mathfrak{t}^2 - 1)x + 1 = -(x^2 - (\mathfrak{t}^2 - 2)x + 1)(x - 1), \mathfrak{t} = \text{tr}\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix}\right),$$

which leads to the eigenvalues

$$1, \frac{\mathfrak{t}^2 - 2 \pm \mathfrak{t}\sqrt{\mathfrak{t}^2 - 4}}{2} = \left(\frac{\mathfrak{t} \pm \sqrt{\mathfrak{t}^2 - 4}}{2}\right)^2.$$

In particular, the eigenvalues are squares of numbers in the quadratic number field affiliated with the discriminant. This has the interesting consequence that the matrix $\Psi(\mathfrak{F})$ has a square root in the ring of matrices with entries from that number field. The identity (10.3) can now be recast as follows,

$$\begin{aligned} & \begin{pmatrix} \omega\lambda^n + \omega^*\lambda^{-n} & 3\omega^2\lambda^{2n+1} + 3(\omega^*)^2\lambda^{-(2n+1)} + \tau & \omega\lambda^{n+1} + \omega^*\lambda^{-(n+1)} \\ \omega\varrho\lambda^n + \omega^*\varrho^*\lambda^{-n} & 3\omega^2\varrho\lambda^{2n+1} + 3(\omega^*)^2\varrho^*\lambda^{-(2n+1)} + \frac{1}{2}(\varrho + \varrho^*)\tau & \omega\varrho\lambda^{n+1} + \omega^*\varrho^*\lambda^{-(n+1)} \\ \omega\varrho^2\lambda^n + \omega^*(\varrho^*)^2\lambda^{-n} & 3\omega^2\varrho^2\lambda^{2n+1} + 3(\omega^*)^2(\varrho^*)^2\lambda^{-(2n+1)} + \varrho\varrho^*\tau & \omega\varrho^2\lambda^{n+1} + \omega^*(\varrho^*)^2\lambda^{-(n+1)} \end{pmatrix} - 1 \\ & = \frac{1}{2} \begin{pmatrix} \omega\varrho^2\lambda^n + \omega^*(\varrho^*)^2\lambda^{-n} & -2(\omega\varrho\lambda^n + \omega^*\varrho^*\lambda^{-n}) & \omega\lambda^n + \omega^*\lambda^{-n} \\ -\varrho\varrho^*\mathfrak{b} & (\varrho + \varrho^*)\mathfrak{b} & -\mathfrak{b} \\ \omega\varrho^2\lambda^{n+1} + \omega^*(\varrho^*)^2\lambda^{-(n+1)} & -(\omega\varrho\lambda^{n+1} + \omega^*\varrho^*\lambda^{-(n+1)}) & \omega\lambda^{n+1} + \omega^*\lambda^{-(n+1)} \end{pmatrix} \\ & + \frac{3}{2} \begin{pmatrix} \omega\varrho\lambda^n + \omega^*\varrho^*\lambda^{-n} & \omega\lambda^n + \omega^*\lambda^{-n} & 0 \\ 0 & 0 & 0 \\ -(\omega\varrho\lambda^{n+1} + \omega^*\varrho^*\lambda^{-(n+1)}) & -(\omega\lambda^{n+1} + \omega^*\lambda^{-(n+1)}) & 0 \end{pmatrix}, \end{aligned}$$

where $\tau = \frac{4\mathfrak{b}}{9\mathfrak{b}^2-4}$, and it can be proved algebraically (disregarding the integrality of the entries involved) by employing the norm form equation, as well as an identity relating the quantities ω and ϱ ,

$$\omega\omega^* = \frac{\mathfrak{b}^2}{9\mathfrak{b}^2-4} = \frac{1}{(\varrho - \varrho^*)^2}.$$

In the context of the example in the third remark at the end of Section 1, if (A, AB, B) is an admissible triple such that

$$AB = \begin{pmatrix} k_b & 3k_b - l_b \\ \mathfrak{b} & 3\mathfrak{b} - k_b \end{pmatrix} = \begin{pmatrix} k_b & -l_b \\ \mathfrak{b} & -k_b \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix},$$

then,

$$\begin{aligned} A &= \begin{pmatrix} \omega\varrho_+\lambda + \omega^*\varrho_+^*\lambda^{-1} & 3(\omega\varrho_+\lambda + \omega^*\varrho_+^*\lambda^{-1}) - (\omega\varrho_+^2\lambda + \omega^*(\varrho_+^*)^2\lambda^{-1}) \\ \omega\lambda + \omega^*\lambda^{-1} & 3(\omega\lambda + \omega^*\lambda^{-1}) - (\omega\varrho_+\lambda + \omega^*\varrho_+^*\lambda^{-1}) \end{pmatrix} \\ &= \begin{pmatrix} \omega\varrho_+\lambda + \omega^*\varrho_+^*\lambda^{-1} & -(\omega\varrho_+^2\lambda + \omega^*(\varrho_+^*)^2\lambda^{-1}) \\ \omega\lambda + \omega^*\lambda^{-1} & -(\omega\varrho_+\lambda + \omega^*\varrho_+^*\lambda^{-1}) \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} B &= \begin{pmatrix} \omega\varrho_- + \omega^*\varrho_-^* & 3(\omega\varrho_- + \omega^*\varrho_-^*) - (\omega\varrho_-^2 + \omega^*(\varrho_-^*)^2) \\ \omega + \omega^* & 3(\omega + \omega^*) - (\omega\varrho_- + \omega^*\varrho_-^*) \end{pmatrix} \\ &= \begin{pmatrix} \omega\varrho_- + \omega^*\varrho_-^* & -(\omega\varrho_-^2 + \omega^*(\varrho_-^*)^2) \\ \omega + \omega^* & -(\omega\varrho_- + \omega^*\varrho_-^*) \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

This identity shows in a very explicit way the change of sign, here encoded in the term ϱ_\pm , from "+" on the left, to "-" on the right, where $\mathfrak{b} = \frac{1}{3} \text{tr}(AB)$ is the dominant Markoff number.

References

- [AO] H. Appelgate, H. Onishi, "The similarity problem for 3x3 integer matrices", Linear Algebra Appl. 42 (1982), 159-174
- [Ba] P. Bachmann, "Zahlentheorie", B. G. Teubner, Leipzig 1898, Vierter Teil, Erste Abteilung
- [Bo] E. Bombieri, "Continued fractions and the Markoff tree", Expositiones Mathematicae 25 (3) (2007), 187-213
- [Bu] D. A. Buell, "Binary quadratic forms", Springer Verlag, 1989

- [BV] J. Buchmann, U. Vollmer, “Binary quadratic forms. An algorithmic approach”, Springer Verlag, 2007
- [Ca] J.W.S. Cassels, “An introduction to Diophantine Approximation”, Cambridge Univ. Press, 1957 (Chapter II)
- [CV] S. Cecotti, C. Vafa, “On the classification of N=2 Supersymmetric Theories”, Commun. Math. Phys. 158 (1993), 569-644
- [Co] H. Cohn, “Markoff Forms and Primitive Words”, Math. Ann. 196 (1972), 8-22
- [CF] T.W. Cusick, M.E. Flahive, “The Markoff and Lagrange spectra”, Mathematical Surveys and Monographs, 30, American Mathematical Society (1989)
- [F] F.G. Frobenius “Ueber die Markoffschen Zahlen”, Sitzungsberichte der Koeniglichen Preussischen Akademie der Wissenschaften zu Berlin (1913), 458-487 [Gesammelte Abhandlungen, Band III, Springer Verlag]
- [HZ] F. Hirzebruch, D. Zagier, “The Atiyah-Singer Theorem and Elementary Number Theory”, Publish or Perish (1974)
- [L] E. Landau, “Vorlesungen ueber Zahlentheorie”, Verlag von S. Hirzel in Leipzig (1927), Erster Band
- [M1] L. J. Mordell, “On the representation of a binary quadratic form as a sum of squares of linear forms”, Math. Z. 35 (1932), 1-15
- [M2] L. J. Mordell, “Diophantine Equations”, Academic Press, 1969
- [Ne] M. Newman, “Integral Matrices”, Academic Press, 1972
- [Ni] I. Niven, “Integers of quadratic fields as sum of squares” Trans. Amer. Math. Soc. 48 (1940), 405-417
- [Pe] S. Perrine, “L’interpretation matricielle de la theory de Markoff classique”, Int. J. Math. Math. Sci. 32 (2002),no.4, 193-262
- [Pn] O. Perron, “Die Lehre von den Kettenbruechen”, Band I, Dritte Auflage, B. G. Teubner (1954)
- [Po] J.Popp, “The combinatorics of frieze patterns and Markoff numbers”, arXiv:math/0511633
- [R] R. Remak “Ueber indefinite binaere quadratische Minimalformen”, Math. Ann. 92, 3-4 (1924), 155-182
- [Re] C. Reutenauer, “On Markoff’s property and Sturmian words”, Math. Ann. 336 (1) (2006), 1-12
- [Ru] A. N. Rudakov, “The Markov numbers and exceptional bundles on P^2 “, Math. USSR. Izv., 32(1) (1989), 99-102

- [Se] C. Series, “The geometry of Markoff numbers”, Math. Intelligencer 7 (1985), no.3, 20-29
- [St] B. Stolt, “On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, Part II”, Arkiv för Matematik 2 (10) (1952), 251-268
- [W] M. Waldschmidt, “Open Diophantine Problems”, Moscow Mathematical Journal 4 (2004), no.1, 245-305
- [Za] D. Zagier, “On the Number of Markoff Numbers Below a Given Bound”, Mathematics of Computation, 39 (1982), no.160, 709-723
- [Zh] Y. Zhang, “An elementary proof of Markoff conjecture for prime powers” arXiv:math.NT/0606283

Department of Mathematics
Tulane University
New Orleans, LA 70118
e-mail: nriedel@tulane.edu